The GOLDEN BOOK

of a Raspberry Pi USB Server

Simple Effective Home Pi Server Setup

Dated: 09 February 2021
By: Duckie Hellfire (Youtube)

Warning: This is just an example guide, collected from the net and a few add in of my own. Use at own risk. The setup is for HOME experimental uses behind your existing internet router and firewall and not a replacement router. Use at own risk.

Features: (USB Server)

* ***RaspAP*** *(Wireless Access Point Hotspot)*
* ***Cups & AirPrint*** *(USB Print Server)*
* ***Samba*** *(File Server & Windows Printing)*
* ***Log2Ram*** *(Save your USB or SD by logging to Ram)*
* ***UFW*** *(Raspberry Preferred Firewall)*
* ***CCTV*** *(Webcam Monitor and Notifications)*
* ***SMTP*** *(MSMTP and MUTT Email Notifications)*
* ***Pi-Hole*** *(DNS Blackhole for Adverts and Telemetry and other nasty stuff)*
* ***Unbound*** *(Local DNS Server)*
* ***Anti-Virus*** *(ClamAV scanning and notifications)*
* ***Wifi Off*** *(Switch off the WiFi at times Green Anti-EMF)*
* ***Backups*** *(Backup the Samba shared files to Google Drive)*
* ***Disaster Recovery of the USB*** *(Clone the USB to another)*
* ***File Monitoring*** *(Create Notifications when Samba Shares are getting full)*
* ***Auto System Reboots*** *(Set how often and when the system reboots)*
* ***Health Reports*** *(Collection of Reports places in the samba share and emailed)*

BONUS MATERIAL AT BOTTOM INSTALL KODI, WEBSERVER and SEE YOUR CCTV ON KODI! + REMOTE

SETTING UP THE COMPUTER AND A USB PEN DRIVE

Requirements:

* 1 old computer with network port and is able to boot from USB (I used a Dell Wyse 7010)
* Wireless USB CARD or built in if supported (I used a **RT5370** USB)
* Network Cable (Plugged from the PC to the back of your Internet Router)
* DVI/VGA to TV\Monitor Connection
* Keyboard and Mouse
* USB Memory Stick x2 (I used a Kingston Data Traveler G4 32GB) you can use a HDD or SDD
* 2GB Memory (minimal)

NOTE: In this guide Microsoft Word likes to sometimes change the start of the command line to a capital letter. Linux is case sensitive, so if you see a capital you may need to change it to lower case.

1. First **Download** and install Rufus Portable (Currently 3.13)
https://rufus.ie

2. **Unpack** the ZIP file into in to a folder e.g. C:\Software\Rutus\

3. **Download** Raspberry Pi Desktop OS **ISO** (Debian Buster / Raspberry Pi Desktop)
https://www.raspberrypi.org/software/raspberry-pi-desktop/

4. **Plug in** your **USB** and **start RUFUS**

5. **Select** your USB drive in RUFUS

6. **Select the ISO** Raspberry Buster Desktop

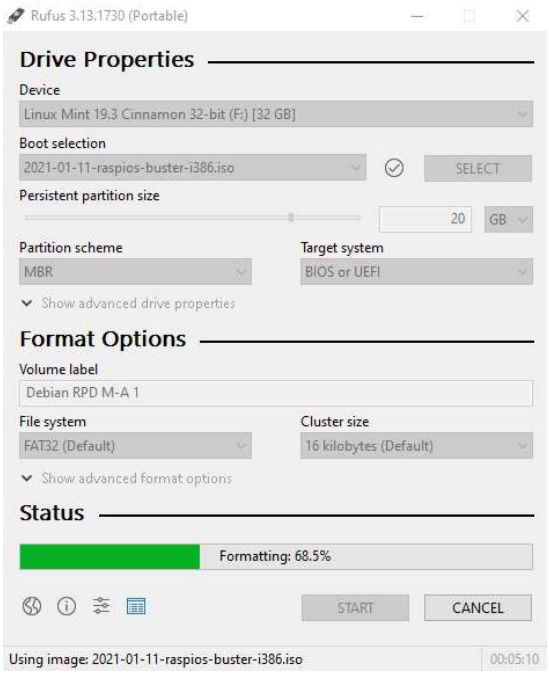
7. Select **Persistent Partition Size** *(I selected 20GB)*
On the slider set **66% of USB** drive size (Keep some space open)

8. Set the Partition Scheme to **MBR** if not already selected

9. Leave all other settings as **default**

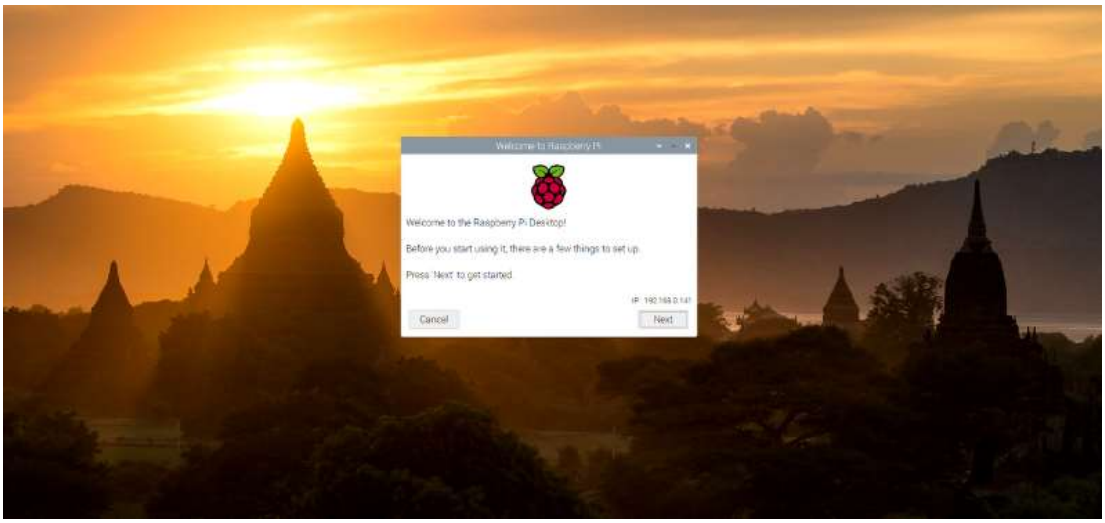
10. **WARNING: THIS WILL DESTROY ALL DATA ON THE SELECTED DRIVE**
Press Start

11. **Have a coffee and wait** for it to finish (takes some time)



Finished

CONNECT EVERYTHING AND START THE COMPUTER


Welcome to Raspberry Pi
Welcome to the Raspberry Pi Desktop!
Before you start using it, there are a few things to set up.
Press 'Next' to get started.
Cancel
Next

(Make sure your LAN cable is connect to your router and issued a DHCP IP address automatically)

1. Plug in the following to the computer
   *** Keyboard and Mouse**
   *** The DVI \ VGA cable into the Monitor**
   *** The Network Cable**
   *** The Webcam**
   *** The Printer USB Cable**
   *** The Wireless USB Dongle**
   *** The USB Dongle with the Raspberry Pi Buster system Installed**

2. When your computer boots make sure the computer **BOOT ORDER** is set to boot from the USB and make sure the **LAST STATE** is set in case of power outages in the **Computer Bios**.

3. Once your computer has booted you should be greeted by the Raspberry Pi Desktop screen, Please note the **IP <ADDRESS>** shown at the bottom right of the setup screen

4. Click **NEXT**

5. Select your **REGION**, **LANUAGE** and **TIME ZONE**

6. Make sure to **CLICK** the **OPTION** "**Use English Language**"

7. Click **NEXT**

8. The OS will now save your settings for a second

9. You are now asked to change the password
   (No need to change the password now, it's up to you)

10. Click **SKIP**

11. You will be asked to "**SELECT WIFI NETWORK**"
    (Do not setup the WiFI network, there is no need, we do this later and work with eth network)
    If you are not going to use the ETH connector and want WIFI and skip a few things then ok set it)

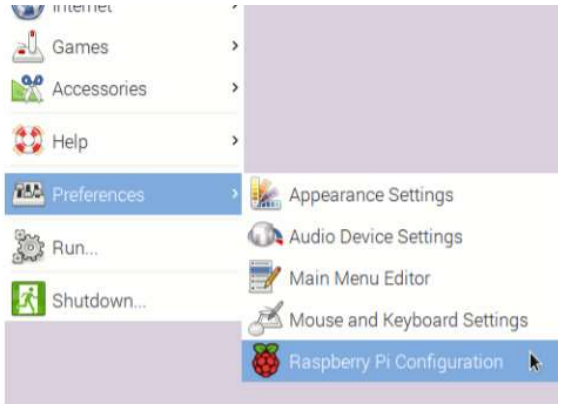
12. Click **SKIP**

13. You will now be asked to "UPDATE THE SOFTWARE"
    (This can take very long and we will be doing this later)

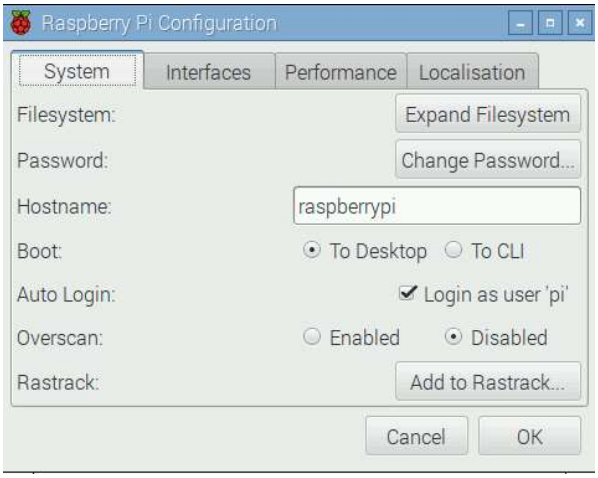
14. Click **SKIP**

15. Click **DONE**

16. Next click on the **Raspberry Desk Menu** (This is the Raspberry on the top left corner of desktop)
Select -> Preferences
Select -> Raspberry Pi Configuration



17. On the **SYSTEM** tab click



Boot -> **To CLI** (We won't need the Desktop and its faster without the desktop)
Auto Login -> **DISABLED** (We do not want to automatically login as user PI)

18. On the **INTERFACES** tab click
SSH -> **ENABLED**

Click **OK** (at the bottom)

Continue to the next page

Now we need to FIX (WORK AROUND) a SSH Problem with the USB Stick
For some reason or permissions or certificate we need to lower the security.
Note this is a work around and should not be used over the internet
https://askubuntu.com/questions/204400/ssh-public-key-no-supported-authentication-methods-available-server-sent-publ

Open the **TERMINAL** on the **RASPBERRY PI DESKTOP**

1. We need to edit the **sshd_config** file

```
sudo nano /etc/ssh/sshd_config
```

2. Change the follow lines from "**no**" to "**yes**" in this file

```
##########################################
PasswordAuthentication yes
ChallengeResponseAuthentication yes
##########################################
```

3. to **SAVE** press **CTRL + X** -> **Y** -> **ENTER** key

4. Next we want to **reboot** the system, Click the **Raspberry Desktop Menu**
   Select -> **SHUTDOWN**
   Click -> **REBOOT**

Finished

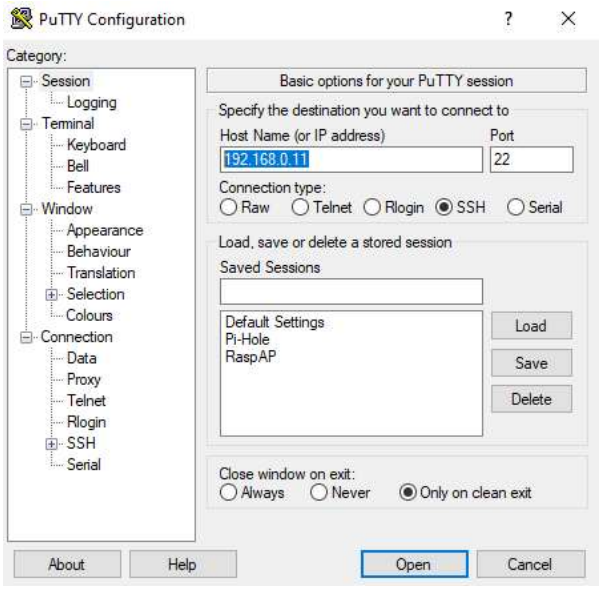
SSH with Putty & Fix (Your first remote login)

Resources Guides:
https://www.howtogeek.com/311287/how-to-connect-to-an-ssh-server-from-windows-macos-or-linux/

Notes:
From a Linux Terminal = ssh username@ssh.server.com or ssh pi@192.168.0.6
Port 22 is used for SSH

Download and install Putty to your Windows PC
https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

After Putty is installed -> **OPEN** Putty



1. Enter the **IP Address** you recorded when you installed the system into Putty and set **Port 22** and click **OPEN**
2. You will be prompted for a PUTTY Security Alert, this is the certificate. CLICK **YES**
3. Enter the **LOGIN AS** Username = pi
4. Enter the Password = raspberry

If you can't get or remember the Ip Address **DHCP** assigned to your computer, go back to your computer and type in **ifconfig**
This will show you eth0 and the IP address assigned to your computer.

SETTING UP A STATIC IP OR DHCP IP ROUTER RESERVATION

Resources Guides:

https://www.raspberrypi.org/documentation/linux/usage/commands.md

Notes: See end of book for wifi setup

passwd (Command to change passwords)

If you intend to install RaspAP (Wireless Access Point) its recommended to do a DHCP Router IP Reservation on your Internet Router with DHCP. RaspAP will remove the Static IP, I do Both in my setup

1. **Edit** the following file to change to a static IP

```
sudo nano /etc/dhcpcd.conf
```

2. **Remove the #** and **enter your desired IP** setup. If you wish to leave it as DHCP do nothing

Below is **an example** yours only needs remove the # and set the IP leave the rest

```
#########################################################################
# Example static IP configuration:
interface eth0
static ip_address=192.168.0.2/24
static ip6_address=fd51:42f8:caae:d92e::ff/64
static routers=192.168.0.1
static domain_name_servers=192.168.0.1 8.8.8.8 fd51:42f8:caae:d92e::1
#########################################################################
```

3. Save your changes **CTRL X** -> **Y** -> **ENTER**

4. Reboot your system

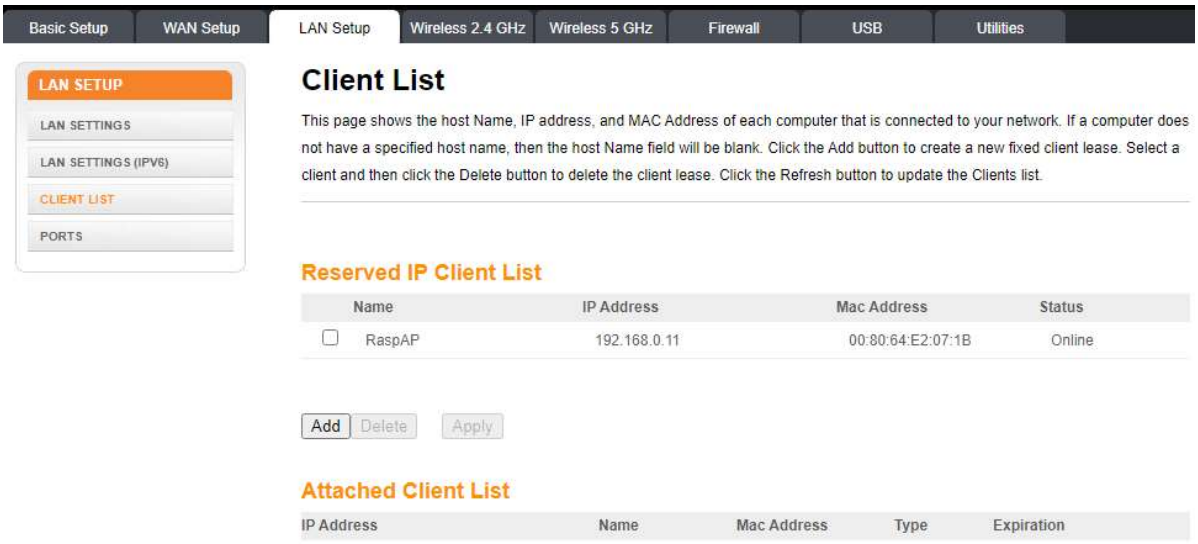
```
sudo reboot
```

Continue to the next page

Entering a DHCP Reservation on your Internet Router

1. **Login to your Internet Router** via a Web Browser, Depending on the IP e.g. http://192.168.0.1

2. Find the **DHCP CLIENT LIST** and **ADD YOUR SYSTEM MAC ADDRES** and **IP ADDRESS** and **HOST NAME** and **APPLY** or **SAFE** the **CHANES**

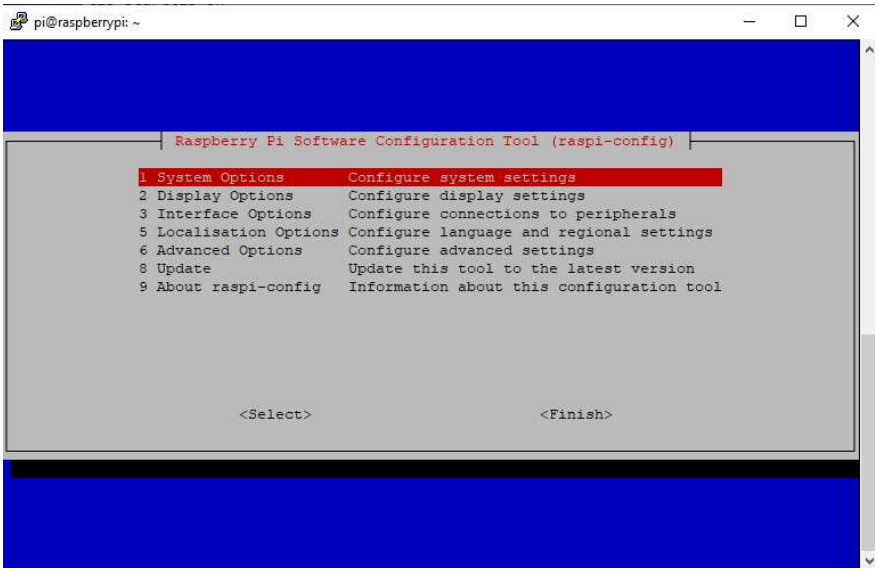


Finished

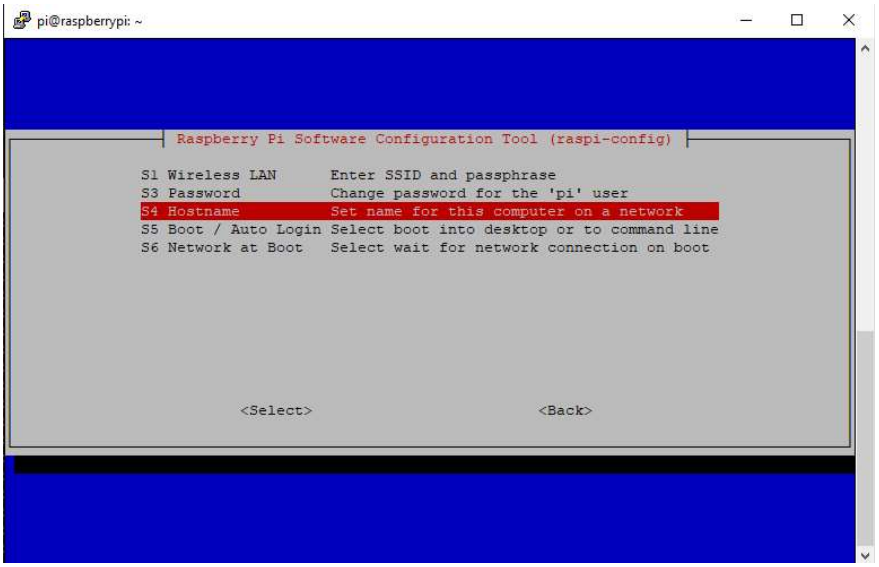
Changing your Computers HOSTNAME

1. To change your hostname on your Computer type **raspi-config**
   sudo raspi-config

2. Select **1. System Option**

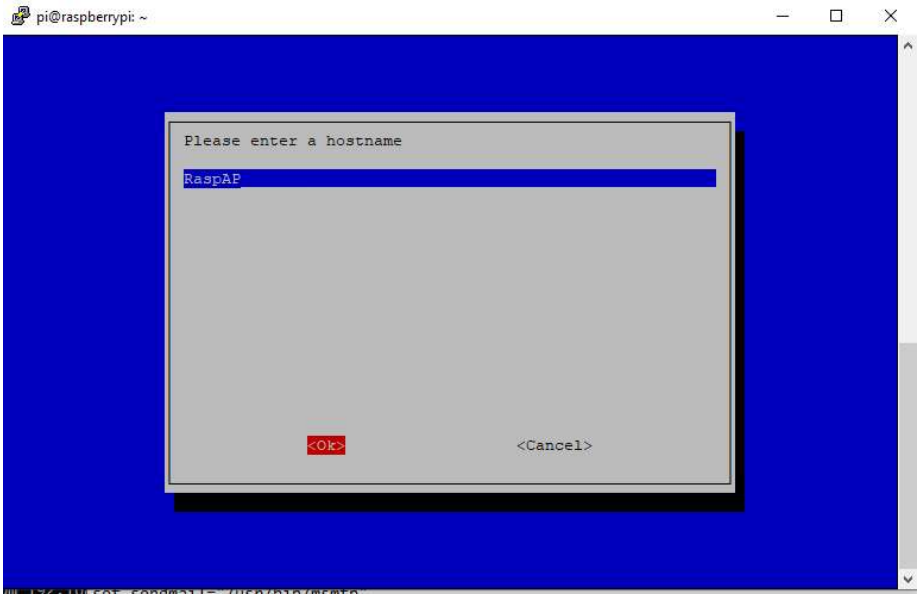

pi@raspberrypi: ~
Raspberry Pi Software Configuration Tool (raspi-config)
1 System Options Configure system settings
2 Display Options Configure display settings
3 Interface Options Configure connections to peripherals
5 Localisation Options Configure language and regional settings
6 Advanced Options Configure advanced settings
8 Update Update this tool to the latest version
9 About raspi-config Information about this configuration tool
<Select>
<Finish>

3. Select **S4 Hostname**


pi@raspberrypi: ~
Raspberry Pi Software Configuration Tool (raspi-config)
S1 Wireless LAN Enter SSID and passphrase
S3 Password Change password for the 'pi' user
S4 Hostname Set name for this computer on a network
S5 Boot / Auto Login Select boot into desktop or to command line
S6 Network at Boot Select wait for network connection on boot
<Select>
<Back>

4. Enter **OK**

5. Enter the new hostname “**RaspAP**”



6. TAB ENTER -> **OK**

7. TAB ENTER -> **FINISH**

8. Would you like to **reboot** TAB ENTER -> **YES**

9. Your system will reboot and you will have a new **HOSTNAME**

Finished

CREATE A FILE IN THE Pi HOME FOLDER TO IDENTIFY THE PC WHEN WE SSH

---

1. You can enter the command **hostname** to see the computer hostname
hostname

2. To change directory to your home folder use **$home** (aka /home/pi)
cd $home

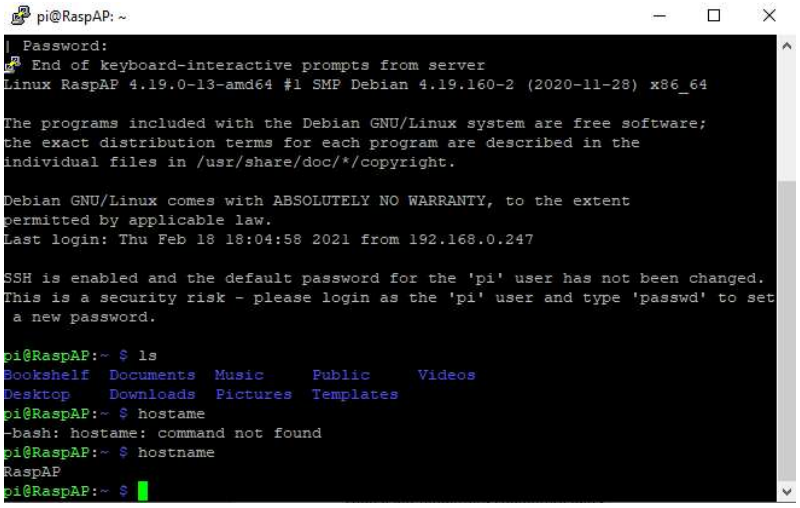
3. You can use **nano** editor and make a file in your home directory
In this case <computername> -> **RaspAP**
sudo nano /home/pi/<computername>

To save the file enter
CTRL X -> **y** -> **ENTER**

4. You can also use **touch** to create a empty file
touch /home/pi/<computername>

5. To see files in directories use the **ls** (Dos is **DIR**)
ls
or
ls -al

This way when you login you can either type in hostname or ls and see the name of your computer you SSH into.


pi@RaspAP: ~
Password:
End of keyboard-interactive prompts from server
Linux RaspAP 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Feb 18 18:04:58 2021 from 192.168.0.247
SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set
a new password.
pi@RaspAP:~ $ ls
Bookshelf Documents Music Public Videos
Desktop Downloads Pictures Templates
pi@RaspAP:~ $ hostame
-bash: hostame: command not found
pi@RaspAP:~ $ hostname
RaspAP
pi@RaspAP:~ $

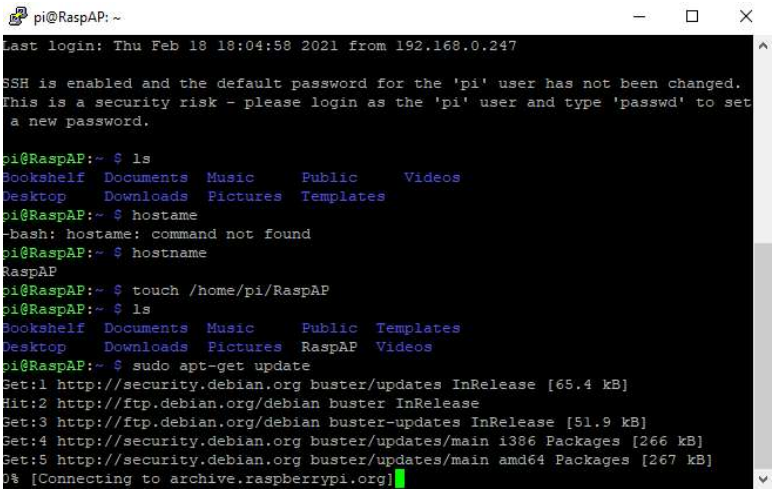
Finished

UPDATE & UPGRADE YOUR SYSTEM

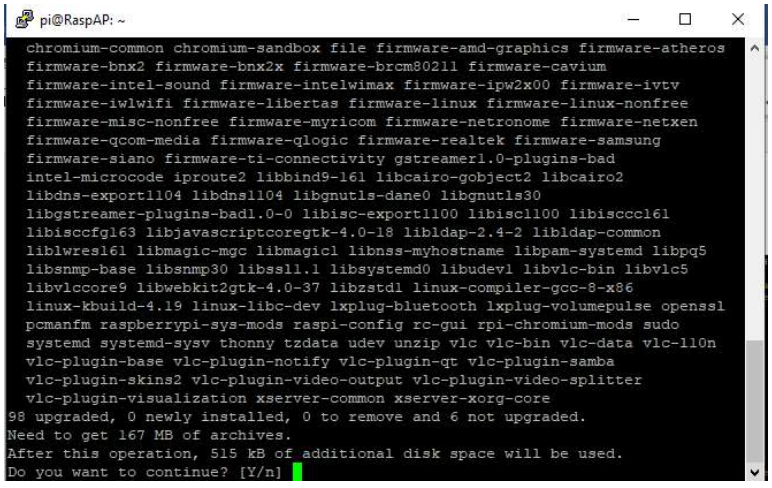
(This could take a long time)

Before we continue we need to **update and upgrade** the **system**

1. First we **update** the system
   sudo apt-get update


pi@RaspAP: ~
Last login: Thu Feb 18 18:04:58 2021 from 192.168.0.247
SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set
a new password.
pi@RaspAP:~ $ ls
Bookshelf Documents Music Public Videos
Desktop Downloads Pictures Templates
pi@RaspAP:~ $ hostame
-bash: hostame: command not found
pi@RaspAP:~ $ hostname
RaspAP
pi@RaspAP:~ $ touch /home/pi/RaspAP
pi@RaspAP:~ $ ls
Bookshelf Documents Music Public Templates
Desktop Downloads Pictures RaspAP Videos
pi@RaspAP:~ $ sudo apt-get update
Get:1 http://security.debian.org buster/updates InRelease [65.4 kB]
Hit:2 http://ftp.debian.org/debian buster InRelease
Get:3 http://ftp.debian.org/debian buster-updates InRelease [51.9 kB]
Get:4 http://security.debian.org buster/updates/main i386 Packages [266 kB]
Get:5 http://security.debian.org buster/updates/main amd64 Packages [267 kB]
0% [Connecting to archive.raspberrypi.org]

2. Next we **upgrade** the system (This may take a very long time)
   sudo apt-get upgrade


pi@RaspAP: ~
chromium-common chromium-sandbox file firmware-amd-graphics firmware-atheros
firmware-bnx2 firmware-bnx2x firmware-brcm80211 firmware-cavium
firmware-intel-sound firmware-intelwimax firmware-ipw2x00 firmware-ivtv
firmware-iwlwifi firmware-libertas firmware-linux firmware-linux-nonfree
firmware-misc-nonfree firmware-myricom firmware-netronome firmware-netxen
firmware-qcom-media firmware-qlogic firmware-realtek firmware-samsung
firmware-siano firmware-ti-connectivity gstreamer1.0-plugins-bad
intel-microcode iproute2 libbind9-161 libcairo-gobject2 libcairo2
libdns-export1104 libdns1104 libgnutls-dane0 libgnutls30
libgstreamer-plugins-bad1.0-0 libisc-export1100 libisc1100 libisccc161
libisccfg163 libjavascriptcoregtk-4.0-18 libldap-2.4-2 libldap-common
liblwres161 libmagic-mgc libmagic1 libnss-myhostname libpam-systemd libpq5
libsnmp-base libsnmp30 libssl1.1 libsystemd0 libudev1 libvlc-bin libvlc5
libvlccore9 libwebkit2gtk-4.0-37 libzstd1 linux-compiler-gcc-8-x86
linux-kbuild-4.19 linux-libc-dev lxplug-bluetooth lxplug-volumepulse openssl
pcmanfm raspberrypi-sys-mods raspi-config rc-gui rpi-chromium-mods sudo
systemd systemd-sysv thonny tzdata udev unzip vlc vlc-bin vlc-data vlc-l10n
vlc-plugin-base vlc-plugin-notify vlc-plugin-qt vlc-plugin-samba
vlc-plugin-skins2 vlc-plugin-video-output vlc-plugin-video-splitter
vlc-plugin-visualization xserver-common xserver-xorg-core
98 upgraded, 0 newly installed, 0 to remove and 6 not upgraded.
Need to get 167 MB of archives.
After this operation, 515 kB of additional disk space will be used.
Do you want to continue? [Y/n]

3. When done **please reboot**
   sudo reboot

SETUP A REBOOT SCHEDULE

Resources Guides:

Notes:
This will allow us to keep the system in prime condition once a week
*You can use **@daily** for everyday in the **crontab***
or
@reboot
---

1. **Run** the following **command** to edit the crontab
   If asked what editor to use select **NANO**

```
sudo crontab -u pi -e
```

2. **Enter** the following line right at the bottom of the file

```
################################
30 6 * * 1 /sbin/shutdown -r now
################################
```

3.Save your changes

4. **Restart** the **CronTab** service

```
sudo service cron restart
```

5. When completed press **CTRL X** to **save** and enter **Y** for yes when prompted and hit **ENTER** to commit

You now will have a **Scheduled job** what will **reboot** your Pi system **once a week**

Finished

LOG2RAM

This will save some space, speed up things and give the SD, USB longer health

Resources Guides:

https://pimylifeup.com/raspberry-pi-log2ram/

Notes: /var/hdd.log #location of backup logs

---

1. Open your terminal console or SSH and change DIR to **$HOME**

```
cd /home/pi or cd $home
```

2. Its recommended to have **rsync** installed *(This may already be installed)*

```
sudo apt install rsync
```

3. **Download** LOG2RAM

```
wget https://github.com/azlux/log2ram/archive/master.tar.gz -O log2ram.tar.gz
```

4. **Extract** the files in log to ram

```
tar xf /home/pi/log2ram.tar.gz
```

5. **Change folder** to log2ram-master

```
cd /home/pi/log2ram-master
```

6. Make the installer **executable** if not already (Looks GREEN=OK Executable)

```
sudo chmod +x install.sh
```

7. **Run** the installer

```
sudo ./install.sh
```

8. Change the configuration from **SIZE=40M** to **SIZE=128M**

```
sudo nano /etc/log2ram.conf
```

```
############################
SIZE=128M
############################
```

9. **Reboot** for effect to take place

```
sudo reboot
```

10. **OPTIONAL**: Check to see if the log file is running and there should also be a new mount

```
df -h
mount
```

UFW (Uncomplicated Fire Wall)

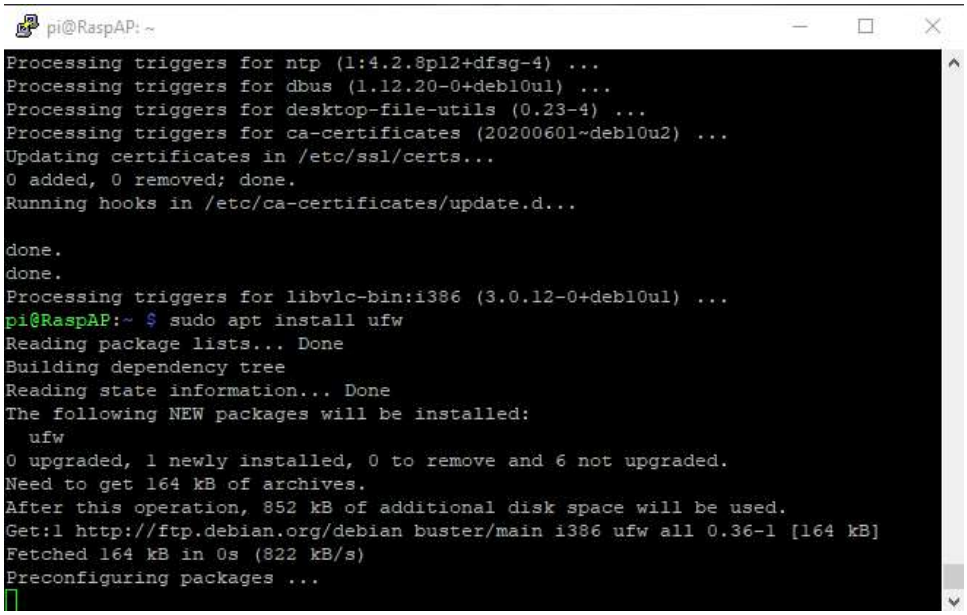
Resources Guides:
https://pimylifeup.com/raspberry-pi-ufw/
https://en.wikipedia.org/wiki/Uncomplicated_Firewall

Notes:
Limits = sudo ufw limit 22
Show Added = sudo ufw show added
sudo ufw allow ssh or sudo ufw allow 22/tcp
Port Ranges = sudo ufw allow 1000:2000/tcp
IPAddress = sudo ufw allow from 192.168.255.255
Deny = sudo ufw deny 80/tcp
sudo ufw delete allow ssh
sudo ufw status numbered
sudo ufw delete [number]
sudo ufw disable
sudo ufw reset

To see what **ports are currently used** run the command **netstat -natp**
sudo netstat -natp
---

1. First **install** the firewall

sudo apt install ufw

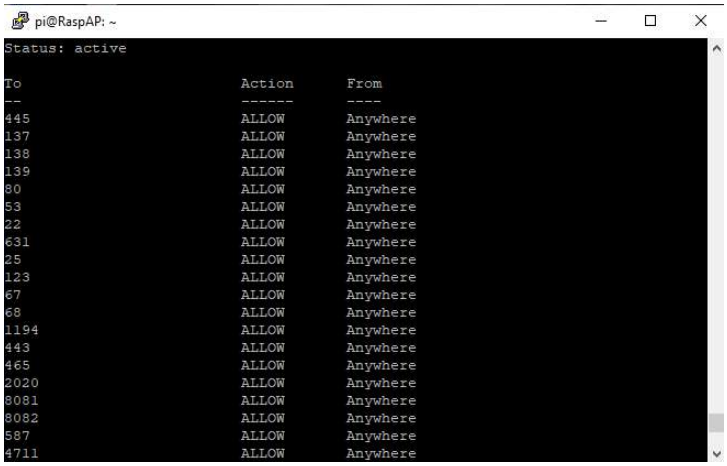

pi@RaspAP: ~
Processing triggers for ntp (1:4.2.8p12+dfsg-4) ...
Processing triggers for dbus (1.12.20-0+deb10u1) ...
Processing triggers for desktop-file-utils (0.23-4) ...
Processing triggers for ca-certificates (20200601~deb10u2) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
done.
Processing triggers for libvlc-bin:i386 (3.0.12-0+deb10u1) ...
pi@RaspAP:~ $ sudo apt install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
ufw
0 upgraded, 1 newly installed, 0 to remove and 6 not upgraded.
Need to get 164 kB of archives.
After this operation, 852 kB of additional disk space will be used.
Get:1 http://ftp.debian.org/debian buster/main i386 ufw all 0.36-1 [164 kB]
Fetched 164 kB in 0s (822 kB/s)
Preconfiguring packages ...

2. Run each **command** to add an open Port **ALLOW**, skips ones you don't need

```
sudo ufw allow 445                  # SAMBA
sudo ufw allow 137                  # SAMBA
sudo ufw allow 138                  # SAMBA
sudo ufw allow 139                  # SAMBA
sudo ufw allow 80                   # Webserver
sudo ufw allow 53                   # DNS
sudo ufw allow 22                   # SSH
sudo ufw allow 631                  # CUPS PRINTER
sudo ufw allow 25                   # SMTP
sudo ufw allow 123                  # Time Services ????
sudo ufw allow 67                   # DHCP
sudo ufw allow 68                   # DHCP
sudo ufw allow 1194                 # OpenVPN
sudo ufw allow 443                  # OpenVPN / HTTPS
sudo ufw allow 465                  # SMTPS
sudo ufw allow 2020                 # (Use only if you are using Raspberry Cast)
sudo ufw allow 8080                 # (CCTV Webcam Monitor)
sudo ufw allow 8081                 # (CCTV Webcam Monitor)
sudo ufw allow 8082                 # (Wifi RaspAP Admin Page after changing from 80)
sudo ufw allow 587                  # GMAIL????????????
sudo ufw allow 4711                 # ?????????
sudo ufw allow 5335                 # Unbound
sudo ufw allow 9100                 # Printing
sudo ufw allow 58000:60000/tcp      # Unbound
sudo ufw allow 53682                # RClone
```

3. Enable the Firewall and check its status

```
sudo ufw enable
sudo ufw status
```



SETUP mSMTP MAILER TO SEND NOTIFICATIONS

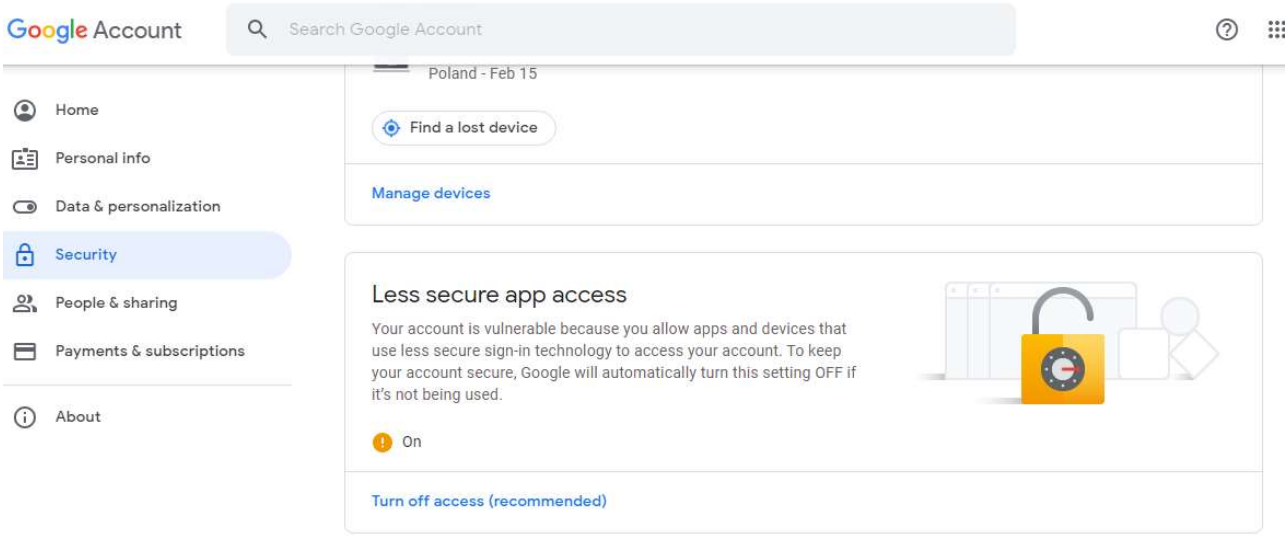
Resources Guides:
https://techrapiduk.blogspot.com/2017/04/send-email-on-raspberry-pi-with-msmtp.html
https://wiki.debian.org/msmtp
https://marlam.de/msmtp/msmtp.html
https://manpages.debian.org/testing/msmtp/msmtp.1.en.html
https://www.computerhope.com/unix/umailx.htm
https://www.binarytides.com/linux-mailx-command/

Notes:
Subject: is the subject of the mail and after \r\n\r\n is the mail's main messages
–debug is the output log of the sending mail
–from=default is which account used for sending the mail
-t username[at]gmail.com is the destination address
---

1. **Create a new Gmail** account for sending mails (Make sure it has a good secure password)

2. Open Gmail **Account Settings**

3. Under Security Enable the option "**Access for less secure apps**" switch on


Google Account
Search Google Account
Home
Personal info
Data & personalization
Security
People & sharing
Payments & subscriptions
About
Poland - Feb 15
Find a lost device
Manage devices
Less secure app access
Your account is vulnerable because you allow apps and devices that use less secure sign-in technology to access your account. To keep your account secure, Google will automatically turn this setting OFF if it's not being used.
On
Turn off access (recommended)

4. **Install** the smtp service on your device with the following command
sudo apt-get install msmtp ca-certificates

5. **Create** the file msmtprc
   sudo touch /etc/msmtprc

6. Next we **edit** the file and enter the settings below.
   Note: Change only the user - email and password to your own Gmail account
   sudo nano /etc/msmtprc

```
################################
account default
host smtp.gmail.com
port 587
logfile /var/log/msmtp.log
tls on
tls_starttls on
tls_trust_file /etc/ssl/certs/ca-certificates.crt

auth login
user youremailaddress@gmail.com
password Yourpassword
from First Last Name

account account2
################################
```

7. Change the file **permissions** with the command below

```
sudo chmod -R 0777  /etc/msmtprc
```

8. Create the log file and set its **permissions**

```
sudo touch /var/log/msmtp.log
sudo chmod -R 0777 /var/log/msmtp.log
sudo chgrp pi /var/log/msmtp.log
```

9. Do a test email and only change the email address at the end to your personal email to send

```
echo -e "Subject: Test Mail\r\n\r\nThis is a test mail" | msmtp --debug --from=default -t
username@gmail.com
```

10. Install a **email client** for attachments called **Mutt** (for file attachments)

```
cd $home
sudo apt-get install mutt
```

OPTIONAL: Encrypt the password
https://manpages.ubuntu.com/manpages/focal/man1/secret-tool.1.html

OPTIONAL TO DO: THE PASSWORD FILE NEEDS ENCRYPTION TO HIDE THE PASSWORD IN THE FILE

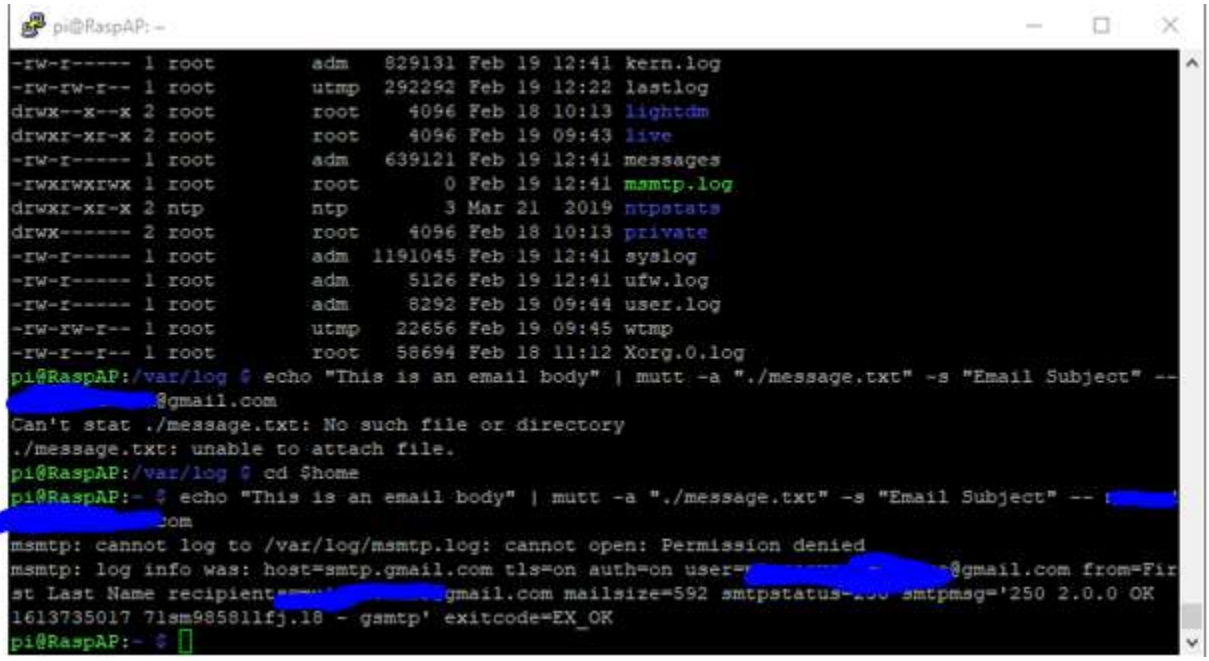
11. **Edit** Mutt config file
sudo nano ~/.muttrc

```
####################################
set sendmail="/usr/bin/msmtp"
set use_from=yes
set from=yournewemail@gmail.com
####################################
```

Save your changes

12. Set the **permissions**
sudo chmod o+rwx /home/pi/.muttrc

13. Test Mutt by sending an **email with attachment (Note permissions of attachments to send)**
echo "Some log event" > message.txt
echo "This is an email body" | /usr/bin/mutt -a message.txt -s "Email Subject" --recipient@gmail.com


pi@RaspAP: ~
-rw-r----- 1 root adm 829131 Feb 19 12:41 kern.log
-rw-rw-r-- 1 root utmp 292292 Feb 19 12:22 lastlog
drwx--x--x 2 root root 4096 Feb 18 10:13 lightdm
drwxr-xr-x 2 root root 4096 Feb 19 09:43 live
-rw-r----- 1 root adm 639121 Feb 19 12:41 messages
-rwxrwxrwx 1 root root 0 Feb 19 12:41 msmtp.log
drwxr-xr-x 2 ntp ntp 3 Mar 21 2019 ntpstats
drwx------ 2 root root 4096 Feb 18 10:13 private
-rw-r----- 1 root adm 1191045 Feb 19 12:41 syslog
-rw-r----- 1 root adm 5126 Feb 19 12:41 ufw.log
-rw-r----- 1 root adm 8292 Feb 19 09:44 user.log
-rw-rw-r-- 1 root utmp 22656 Feb 19 09:45 wtmp
-rw-r--r-- 1 root root 58694 Feb 18 11:12 Xorg.0.log
pi@RaspAP:/var/log $ echo "This is an email body" | mutt -a "./message.txt" -s "Email Subject" --
@gmail.com
Can't stat ./message.txt: No such file or directory
./message.txt: unable to attach file.
pi@RaspAP:/var/log $ cd $home
pi@RaspAP:~ $ echo "This is an email body" | mutt -a "./message.txt" -s "Email Subject" --
msmtp: cannot log to /var/log/msmtp.log: cannot open: Permission denied
msmtp: log info was: host=smtp.gmail.com tls=on auth=on user=
@gmail.com from=Fir
st Last Name recipient=
gmail.com mailsize=592 smtpstatus=
smtpmsg='250 2.0.0 OK
1613735017 71sm985811fj.18 - gsmtp' exitcode=EX_OK
pi@RaspAP:~ $

Finished

SETTING UP PRINTING WITH CUPS & SAMBA

Resources Guides:
https://circuitdigest.com/microcontroller-projects/raspberry-pi-print-server
https://www.tomshardware.com/how-to/raspberry-pi-print-server
https://raspberrytips.com/install-printer-raspberry-pi/
https://www.cups.org/blog/2005-05-10-how-to-restrict-disk-memory-and-cpu-usage.html
https://wiki.debian.org/CUPSDriverlessPrinting

Notes:
Make sure your **printer is ON** and connected to a **USB Port**
---

1. **Install** CUPS with the following command (This may already be installed)
   sudo apt-get install cups

2. After the install we need to **edit** the cupsd.conf file
   sudo nano /etc/cups/cupsd.conf

```
############################################################
# Place these lines right at the top of the file
AutoPurgeJobs Yes
PreserveJobHistory Off
PreserveJobFiles Off
MaxJobs 400
FilterLimit 200

# Look for the following lines and a just them
# Only listen for connections from the local machine.
#Listen localhost:631
Port *:631
Listen /run/cups/cups.sock

# Restrict access to the server...
<Location />
  Order allow,deny
  Allow @Local
</Location>

# Restrict access to the admin pages...
<Location /admin>
  Order allow,deny
  Allow @Local
</Location>
```

```
# Restrict access to configuration files...
<Location /admin/conf>
  AuthType Default
  Require user @SYSTEM
  Order allow,deny
  Allow @Local
</Location>

##########################################################
```

3. Next we need to **restart** the CUPS Service
   sudo service cups restart

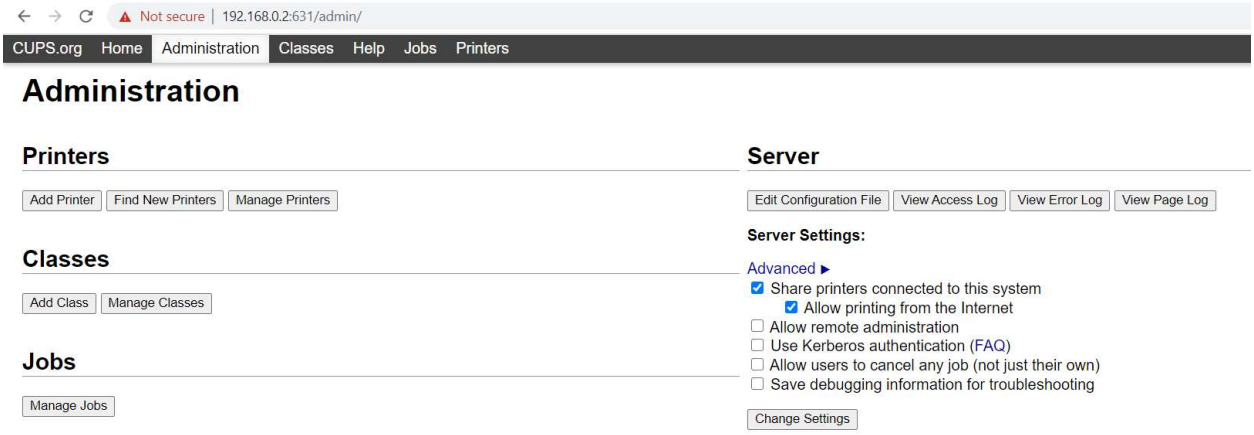
4. We now **add** the pi user to the lpadmin
   sudo usermod -a -G lpadmin pi

5. Configure CUPS so it available over the network
   sudo cupsctl --remote-any

6. Restart CUPS
7. sudo service cups restart

8. We need to do a **test** to see if its working, open your web browser and enter the URL below
   If you are not sure what your IP is type in and look under **eth0**
   Note: At this stage you should have a working printer but we continue to setup
   ifconfig

   http://192.168.0.2:631


Not secure | 192.168.0.2:631/admin/
CUPS.org Home Administration Classes Help Jobs Printers
Administration
Printers
Add Printer Find New Printers Manage Printers
Classes
Add Class Manage Classes
Jobs
Manage Jobs
Server
Edit Configuration File View Access Log View Error Log View Page Log
Server Settings:
Advanced ▸
Share printers connected to this system
Allow printing from the Internet
Allow remote administration
Use Kerberos authentication (FAQ)
Allow users to cancel any job (not just their own)
Save debugging information for troubleshooting
Change Settings

9. Next we **install** Samba for windows printers to work and later for a file server
   sudo apt-get install samba samba-common-bin

10. You will be **asked** if you want to use WINS from the DCHP
    Select Enter on YES

11. **Reboot** the computer
    sudo reboot

12. Next we need to **edit** the smb.conf file and edit the selection below
    sudo nano /etc/samba/smb.conf

```
############################################################
# MAKE SURE YOU ARE IN THE RIGHT SECTION TO CHANGE
[printers]
   comment = All Printers
   browseable = yes
   path = /var/spool/samba
   printable = yes
   guest ok = yes
   read only = no
   create mask = 0700


# printer drivers
[print$]
   comment = Printer Drivers
   path = /var/lib/samba/printers
   browseable = yes
   read only = no
   guest ok = yes
############################################################
```

Save your changes

13. **Restart** the samba services
    sudo service smbd restart

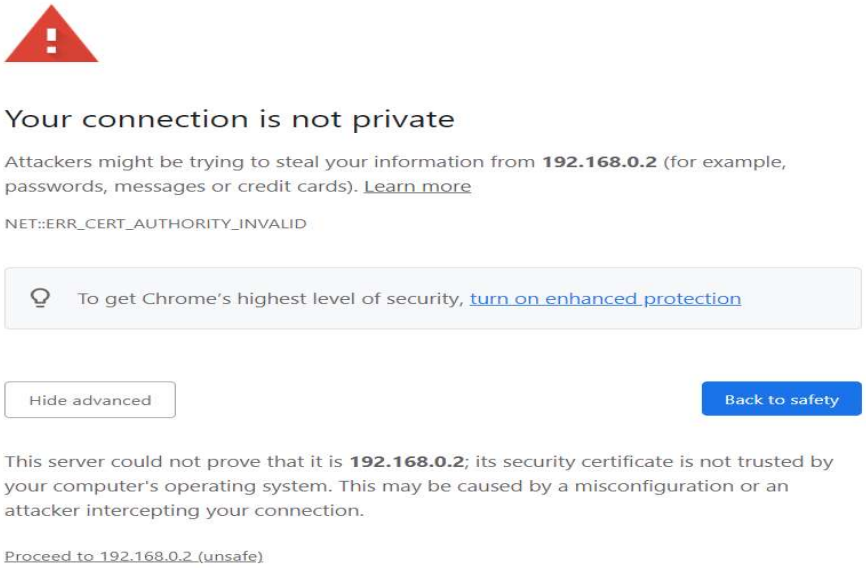
14. Open **CUPS printer URL** page again to add a printer
    http://192.168.0.2:631

    Click on **Administrator Tab**
    Click on **Add Printer**

    You should now get an error UPGRADE REQUIRED
    This is due to no SSL on the page

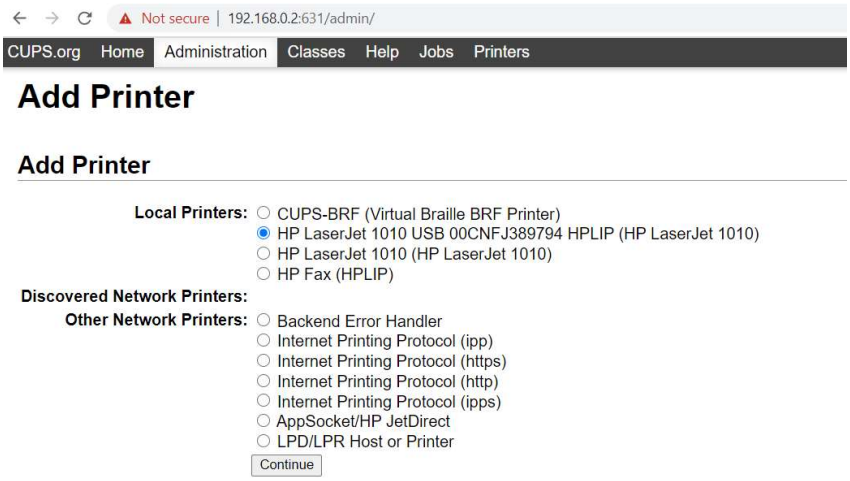
NOTE IN SOME CASES CUPS MAY AUTO DETECT AND SETUP THE PRINTER FOR YOU

15. **Open the page not allowed**


Your connection is not private
Attackers might be trying to steal your information from 192.168.0.2 (for example, passwords, messages or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID
To get Chrome's highest level of security, turn on enhanced protection
Hide advanced
Back to safety
This server could not prove that it is 192.168.0.2; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
Proceed to 192.168.0.2 (unsafe)

16. Next we **add a printer**
    You will be asked to enter your **pi user and password raspberry**

17. Your USB printer should be detected **automatically** under local printers
    Select your printer



18. Select all the **defaults** and click **Share This Printer**

Not secure | 192.168.0.2:631/admin
CUPS.org Home Administration Classes Help Jobs Printers
Add Printer
Add Printer
Name: HP_LaserJet_1010
(May contain any printable characters except "/", "#", and space)
Description: HP LaserJet 1010
(Human-readable description such as "HP LaserJet with Duplexer")
Location:
(Human-readable location such as "Lab 1")
Connection: hp:/usb/hp_LaserJet_1010?serial=00CNFJ389794|HP LaserJet 1010
Sharing: Share This Printer
Continue

19. You can **manage the** printer under Printers when you click on your printer

Not secure | 192.168.0.2:631/printers/
CUPS.org Home Administration Classes Help Jobs Printers
Printers
Search in Printers: Search Clear
Showing 1 of 1 printer.
Queue Name Description Location Make and Model Status
hp-LaserJet-1010 Hewlett-Packard hp LaserJet 1010 RaspAP HP LaserJet 1010, hpcups 3.18.12 Idle

20. Run the following command to **fix a print problem** with hanging and reboot

    lpadmin -p PRINTERNAME -o usb-no-reattach-default=true

    Sudo Reboot

    If for some reason you have problems printing check your samba and other config files have not changed.

Finished

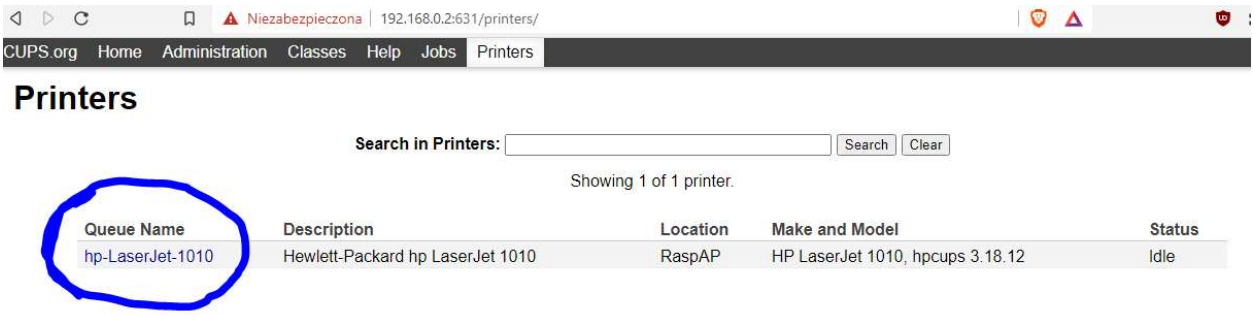
SETUP HPJETDIRECT PORT 9100 PRINTING

Resources Guides:
https://juur.link/2019/01/convert-usb-printer-to-network-printer/

Notes: sudo lpadmin -p HP_LaserJet_1010 -E -v socket://192.168.0.2:9100
I thought I would add this, because everyone is always looking for this
---

1.**Install xinetd**
sudo apt-get install xinetd

2.Go into **CUPS printer admin** and find your printers name you created before
https://192.168.0.2:631/printers/


Niezabezpieczona | 192.168.0.2:631/printers/
CUPS.org Home Administration Classes Help Jobs Printers
Printers
Search in Printers: Search Clear
Showing 1 of 1 printer.
Queue Name Description Location Make and Model Status
hp-LaserJet-1010 Hewlett-Packard hp LaserJet 1010 RaspAP HP LaserJet 1010, hpcups 3.18.12 Idle

3.Edit the **services file** and add the jetdirect port 9100 (may already be added, if not add at the bottom)
sudo nano /etc/services

```
###################################
# Local services
jetdirect      9100/tcp                # laserjet hplj
###################################
```

4.To **start listening on port 9100** edit the following file
sudo nano /etc/xinetd.d/jetdirect

```
# Allow applications using the AppSocket / JetDirect protocol
service jetdirect
{
   socket_type = stream
```

```
    protocol = tcp
    wait = no
    user = lp
Server = /usr/bin/lp
# CHANGE TO YOUR CUPS PRINTER QUEUE NAME example hp-LaserJet-1010
    server_args =  -d hp-LaserJet-1010 -o raw
    groups = yes
    disable = no
}
```

5.Save your file

6.**Restart** the xinetd and cups **service**

```
sudo service xinetd restart
sudo service cups restart
```

You can now print to your printer on port 9100 as a network printer. Below in the workstation printer setup you can see how to print to the printer on windows and in Linux workstation we use CUPS and AppSocket/HP JetDirect

Finished

CONNECTING TO PRINTERS in WINDOWS & LINUX

Resource Guides:
https://en.opensuse.org/SDB:Printing_via_TCP/IP_network

Notes:
In Windows 10 you need to **Enable Windows Discovery** – Follow the Guide below
https://www.thewindowsclub.com/enable-disable-network-discovery-windows

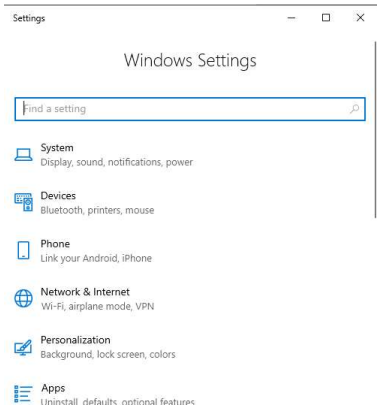
---

PRINTING IN WINDOWS 10 WORKSTATIONS

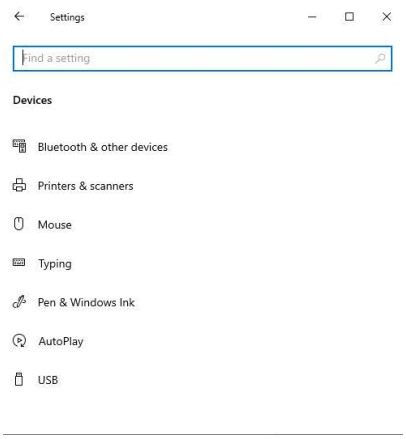
---

1. Click on the Windows start menu and select **Settings**

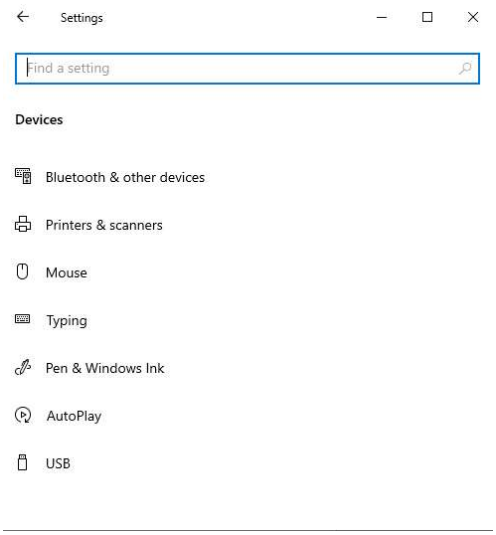
2. Click on **Devices**



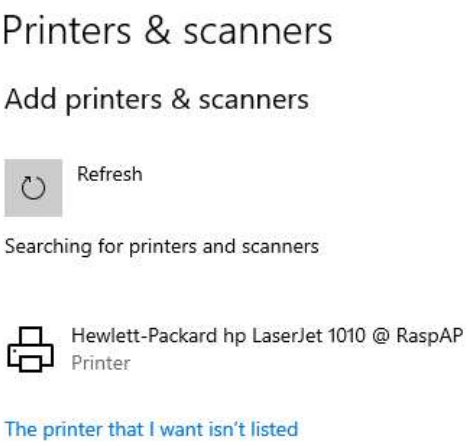
3. Click **Printers and Scanners**



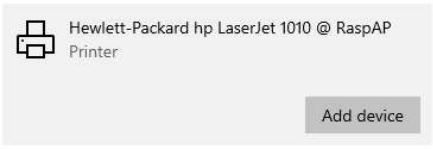
4. Click **Add a Printer or Scanner**



5. The Printer will **automatically** be found



6. Click on the printer and click on **Add Device**



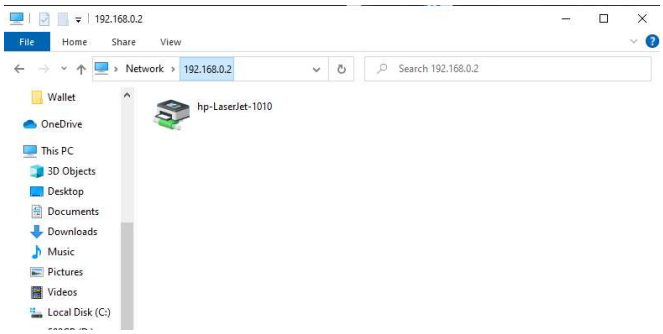
7. The Printer will now be installed and drivers automatically loaded, when finished loading do a test print

---

PRINTERS SETUP IN OTHER MS WINDOWS WORKSTATIONS

We can also install printers from the Samba Share in windows

1. Open **File explorer** and enter your CUPS server IP address in the **address bar** \\192.168.0.2

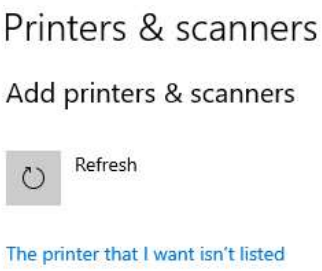


2. Simply **Double Click on the printer** to install it (You may be prompted for a driver)

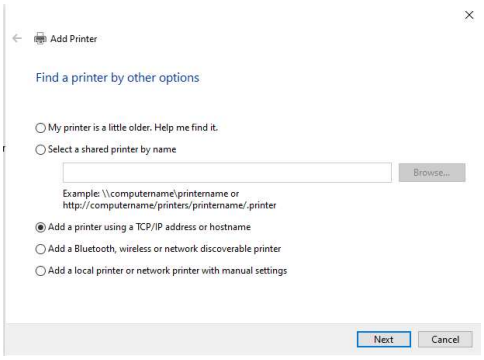
MS WINDOWS JETDIRECT PORT 9100 PRINTER SETUP

---

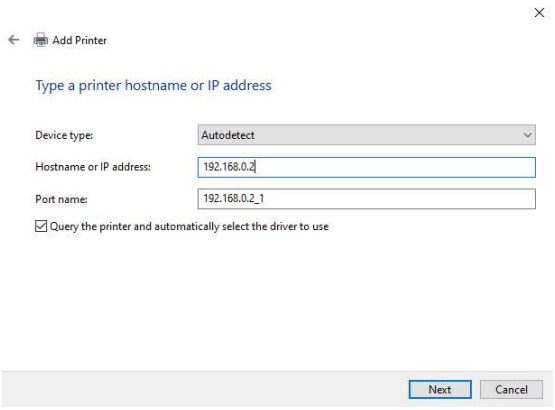
1. Wait for it to stop scanning and select **The printer I want isn't listed**



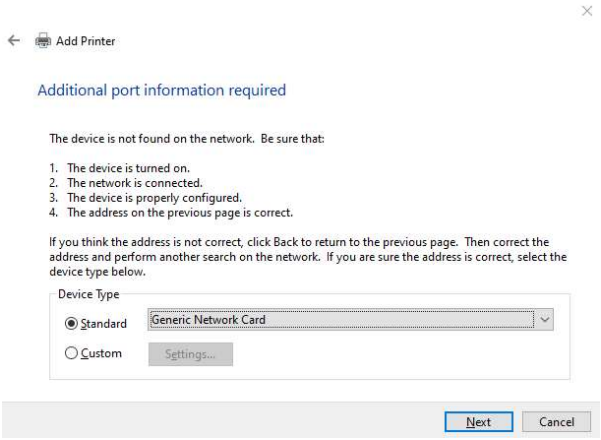
2. Select **Add Printer TCPIP Address**


Add Printer
Find a printer by other options
My printer is a little older. Help me find it.
Select a shared printer by name
Browse...
Example: \\computername\printername or
http://computername/printers/printername/.printer
Add a printer using a TCP/IP address or hostname
Add a Bluetooth, wireless or network discoverable printer
Add a local printer or network printer with manual settings
Next
Cancel

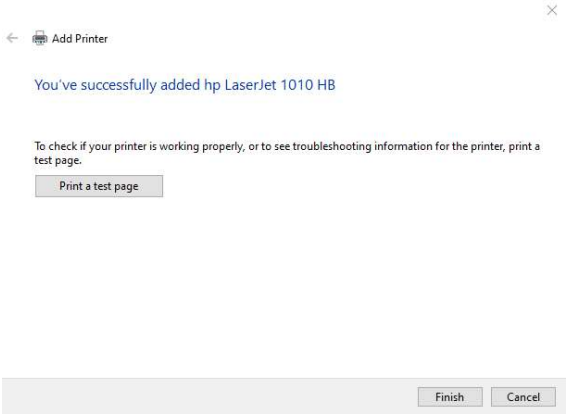
3. Enter your CUPS Printer **IP Address** and click **Next** (e.g. 192.168.0.2)



4. Windows will Detect settings (May be slow)
   When done **select defaults** and click **NEXT**


Add Printer
Additional port information required
The device is not found on the network. Be sure that:
1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.
Device Type
Standard
Generic Network Card
Custom
Settings...
Next
Cancel

5. Windows will next ask for a **Drive**r to be installed
   Select your printers driver and click next next next to **Finish**


Add Printer
You've successfully added hp LaserJet 1010 HB
To check if your printer is working properly, or to see troubleshooting information for the printer, print a test page.
Print a test page
Finish
Cancel

PRINTING SETUP IN LINUX WORKSTATIONS

Resource Guides:
http://www.chschneider.eu/linux/server/cups.shtml

Notes
echo "Hi Network Printer!" | nc 127.0.0.1 9100
echo "Hi POS printer!" > /dev/usb/lp0
cat message.txt > /dev/usb/lp0
---

1. On the Linux Workstation **open your Web browser** with the link below (Cups must be installed on the workstation computer)

   http://localhost:631

2. **Click** on "Add Printer"

3. **Click** on "Add Windows SAMBA Printer"

4. Select **Manufacture and Drivers**

5. Enter the **SAMBA Printer share** option and enter with your **server IP** and **Print Share**
smb://192.168.0.2/hp-LaserJet-1010

6. Do a **test print**

Note or Use *AppSocket/HP JetDirect with port 9100 printers*

Finished

CUPS PRINTERS MAINTANANCE

Resource Guides:
https://www.cups.org/blog/2005-05-10-how-to-restrict-disk-memory-and-cpu-usage.html

Notes:
This **cleans** out any **old printer jobs** twice a day
---

1. **Create** the following files

```
sudo nano /home/pi/CupsMaint.sh
```

2. **Enter** the following in the file

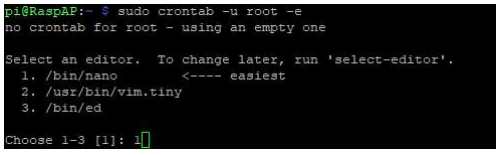
```
################################
#!/bin/bash
sudo service cups stop
sudo rm -f /var/spool/cups/c*
sudo rm -f /var/spool/cups/tmp/*
sudo service cups start
################################
```

3. Make the file **executable**

```
sudo chmod +x /home/pi/CupsMaint.sh
```

4. **Enter** the following at the bottom of the **crontab** to **schedule** the **job** twice a day

```
sudo crontab -u pi -e
```


pi@RaspAP:~ $ sudo crontab -u root -e
no crontab for root - using an empty one
Select an editor. To change later, run 'select-editor'.
1. /bin/nano <---- easiest
2. /usr/bin/vim.tiny
3. /bin/ed
Choose 1-3 [1]: 1

```
################################
0 7 * * * /home/pi/CupsMaint.sh
0 18 * * * /home/pi/CupsMaint.sh
################################
```

5. When done **save** and exit

6. **Restart** the **CronTab** service

```
sudo service cron restart
```

SETTING UP AIRPRINT

Resource Guides:
https://pimylifeup.com/raspberry-pi-airprint/

Notes:
This is for Apple Devices to print
---

1. Let's **install** AirPrint (This may already be installed)

```
sudo apt install avahi-daemon
```

2. When done **Reboot** the system

```
sudo reboot
```

Finished

SETTING UP ANDOIRD SMARTPHONES TO PRINT

Resource Guides:

PrinterShare Mobile Print (Tested and working)
https://play.google.com/store/apps/details?id=com.dynamixsoftware.printershare

NokoPrint - WiFi, Bluetooth, USB printing
https://play.google.com/store/apps/details?id=com.nokoprint

Notes:
Apps are in the Google Play Store

Install the app and search for the printer and print. You may be asked to install a generic driver. OK
If problems search the samba work group and select the printer in there

Finished

SAMBA FILE SHARING SERVER

Resource Guides:
https://lefkowitz.me/setup-a-network-share-via-samba-on-your-raspberry-pi/
https://magpi.raspberrypi.org/articles/samba-file-server
https://en.opensuse.org/SDB:Printing_via_SMB_%28Samba%29_Share_or_Windows_Share
https://www.looklinux.com/how-to-mount-samba-share-smbfs-in-linux/

Notes:
#mount -t (will show you what vfat is mounted)
umount <Partition> will unmount the drive or partition
lpinfo -v
---

1. Let's make a **folder** what will be the root of the file share (Remember Linux is case sensitive)

```
sudo mkdir -m 1777 /share
```

2. Next we **edit** the smb.conf

```
sudo nano /etc/samba/smb.conf
```

3. **Paste** this next section at the bottom of the smb.conf file

```
##############################################
[share]
comment = Share
path = "/share"
browseable = yes
writeable = yes
read only = no
only guest = no
create mask = 0777
directory mask = 0777
public = yes
guest ok = yes
force user = pi
##############################################
```

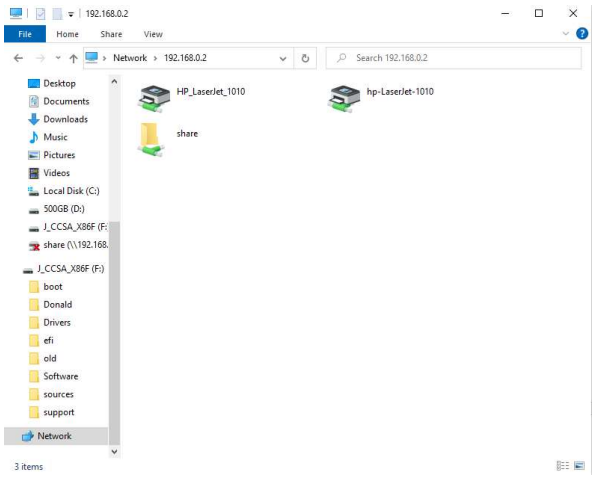
4. When done **save** and exit

5. Now **restart** the samba services

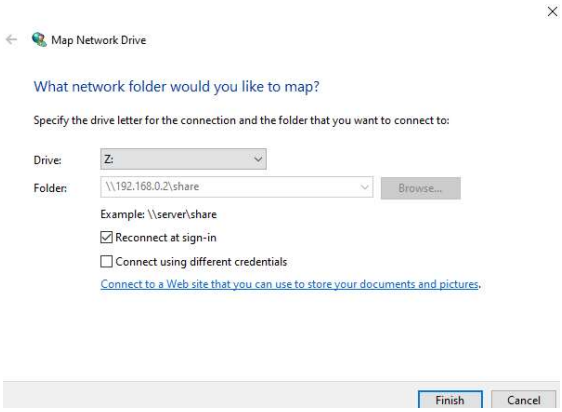
```
sudo systemctl restart smbd
```

6. Now test and open the share in File Explorer in Windows
Enter in the address bar your servers IP Address like below

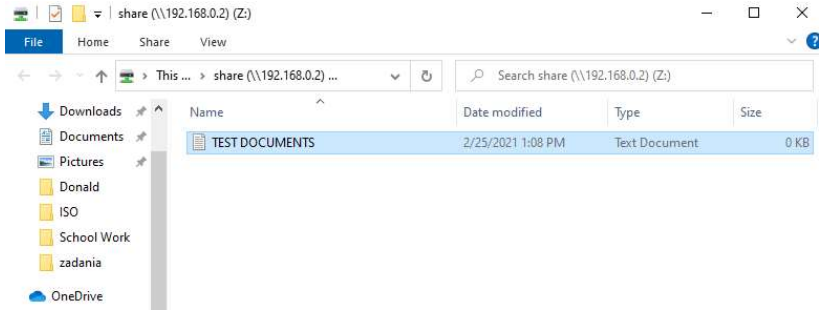
```
\\192.168.0.2
```



7. You now will see the **folder share** and the **printers**
   Right Click on the folder called **"share"**
   Select from the menu "Map Network Drive"
   Select the drive letter (Z) or other and click on **FINISH**


Map Network Drive
What network folder would you like to map?
Specify the drive letter for the connection and the folder that you want to connect to:
Drive:
Z:
Folder:
\\192.168.0.2\share
Browse...
Example: \\server\share
Reconnect at sign-in
Connect using different credentials
Connect to a Web site that you can use to store your documents and pictures.
Finish
Cancel

8. You now will have a **drive** called **Z:** what is a **network share** between all users
   Test the folder by creating a file inside, if any problems check your config file.



CONNECTING LINUX WORKSTATION TO THE NETWORK SHARE

---

1. **Create** a share on the Linux workstation

```
sudo mkdir /Share
```

2. **Mount** the share to the network share

```
mount -t cifs -o username=pi,workgroup=workgroup,password=raspberry //192.168.0.2/share /Share/
```

3. **Edit** the fstab so the mount is connected each time the workstation is rebooted

```
sudo nano /etc/fstab
```

```
########################################################################
//192.168.0.2/share   /Share    cifs  rw,user,username=pi,password=raspberry 0 0
########################################################################
```

4. When done **Save** and continue

5. Create a **symbolic link** (shortcut) to the user's desktop

```
ln -s /Share /home/pi/desktop/Share
```

6. Now the user will have the **Network Share** on his desktop

Finished

SAMBA FILE SHARE MONITORING

Resource Guides:

Notes: This will allow us to monitor the space on the share

---

1. Create the following files (Change the VAR3 to start alerting)

sudo nano /home/pi/spacewarn.sh

```
#############################################################################
#!/bin/bash
# THIS SECTION CHECKS THE SAMBA SHARE AND CREATES A WARNING FILE IF ITS REACHED IT LIMIT
# IT DOES NOT STOP USERS ADDING MORE FILES
   var1=`du -s /share | cut -f 1` # Gets the Bites used for folder
   var2=1024 # Divide Bytes to get the MB
   var3=5000 # Change here to set Warning Limit in MB Currently set to 5GB
   var4=$((var1 / var2)) # Divide the Bites to get MB Sum

if (($var4 < $var3))
then
FILE=/share/WARNING-SHARE-FULL-REDUCE-FILES.txt
if test -f "$FILE"; then
sudo rm /share/WARNING-SHARE-FULL-REDUCE-FILES.txt
fi
fi

if (($var4 > $var3))
then
printf "SHARE FOLDER IS FULL\n \n---------- \nSPACE USED = $var4 MB \n----------\nSPACE
LIMIT = $var3 MB \n----------\n \nPLEASE REDUCE FILES" > /share/WARNING-SHARE-FULL-
REDUCE-FILES.txt
sudo chown pi /share/ WARNING-SHARE-FULL-REDUCE-FILES.txt
#####################################################################
# EMAIL SECTION REMOVE HASH SIGN TO ACTIVATE AND CHANGE EMAIL ADDRESS BELOW
# echo -e "Subject: RaspAP Share Full\r\n\r\nRaspberry Pi Server RaspAP Samba Share is full with $var4
MB" | msmtp --debug --from=default -t recipient@gmail.com
#####################################################################
fi

#############################################################################
```

2. When done **Save** and continue

3. Make the file **executable**

```
sudo chmod +x /home/pi/spacewarn.sh
```

4. Enter the **crontab** to enter the scheduled job
   We create a check every hour

```
sudo crontab -u pi -e
```

```
################################
*/59 * * * * /home/pi/spacewarn.sh
################################
```

5. When done **Save** and continue

7. **Restart** the **CronTab** service

```
sudo service cron restart
```

Finished

CONNECTING TO YOUR FILE SERVER (ANDROID)

Resource Guides:

Notes:
To see your files from your smart phone
Visit the google play store

CX FILE EXPLORER

https://play.google.com/store/apps/details?id=com.cxinventor.file.explorer&hl=en&gl=US

1. Click on **NETWORK**
2. Click on the big **PLUS +**
3. Click on **REMOTE**
4. Click on **LOCAL NETWORK**
5. Click on your **server name** (RASPAP)
6. Select **ANONYMOUS**
7. Click on **OK**
8. You now should have access to the **SHARE**

Finished

BACKUP ONLINE SAMBA FILE SHARE - GOOGLE

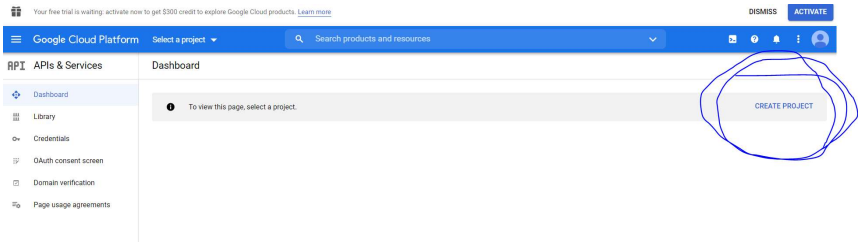
Resource Guides:
https://rclone.org/install/
https://medium.com/@artur.klauser/mounting-google-drive-on-raspberry-pi-f5002c7095c2
https://medium.com/@shubhankarranade30/raspberry-pi-as-nas-with-automated-backup-to-cloud-95be588ed3e5

Notes:
We backup the shared drive so we don't lose our work in a disaster
http://127.0.0.1:53682/Auth
sudo nano $HOME/.config/rclone/rclone.conf
sudo nano root/.config/rclone/rclone.conf
sudo rclone config (Use this to refresh expired tokens if needed)

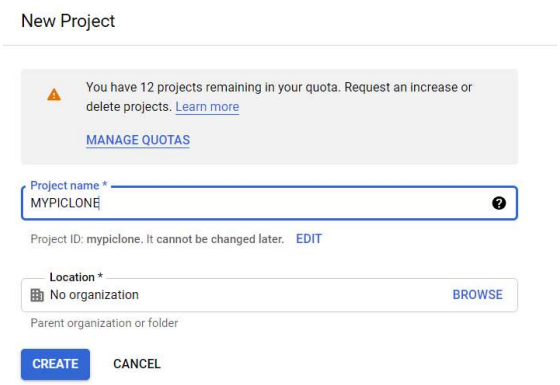
1.Install RCLONE
sudo apt-get install rclone

2.Get a Google Drive Client ID
https://console.developers.google.com/

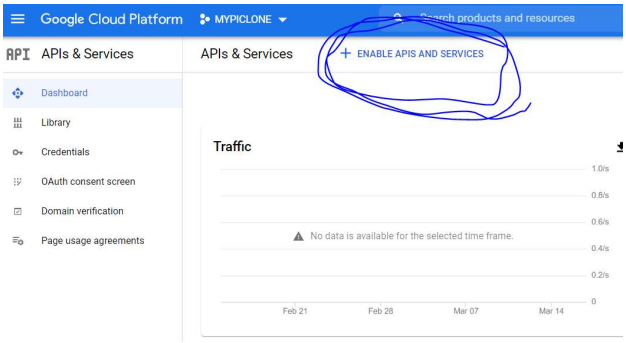
3.Login and Click on CREATE PROJECT



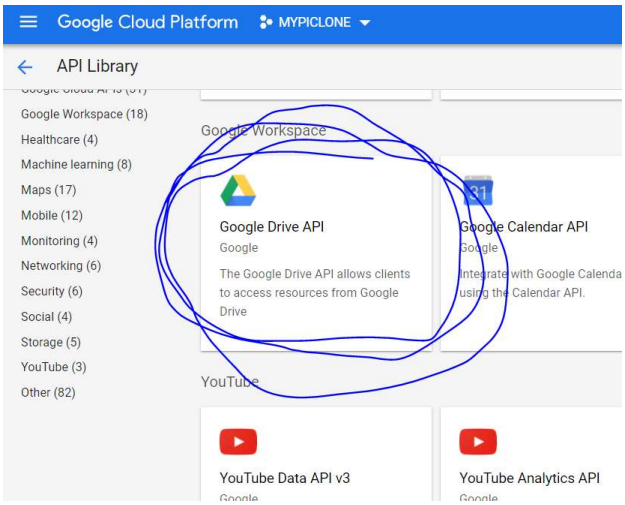
4.Give your project a **name** and click **create**.



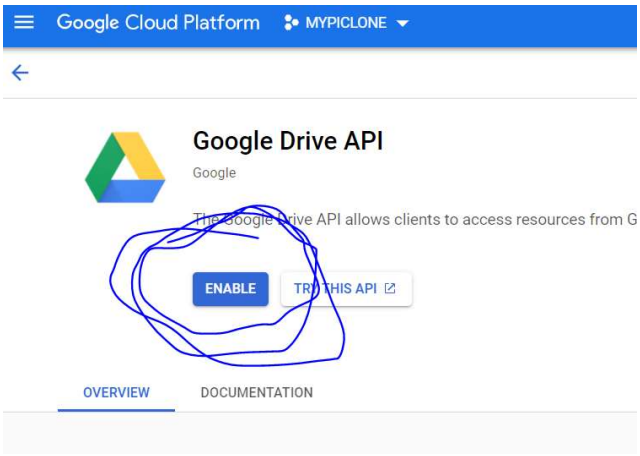
6. Click on **ENABLE APIS AND SERVICES**



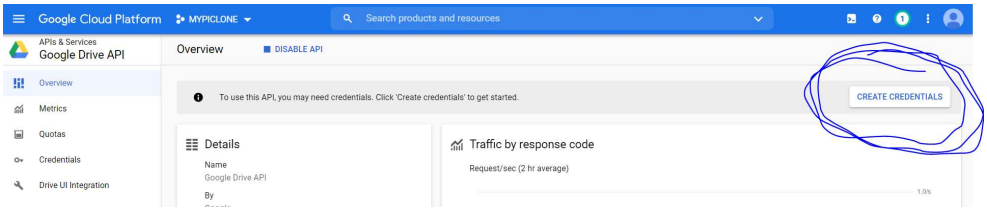
7. Search and Click on **GOOGLE DRIVE API**



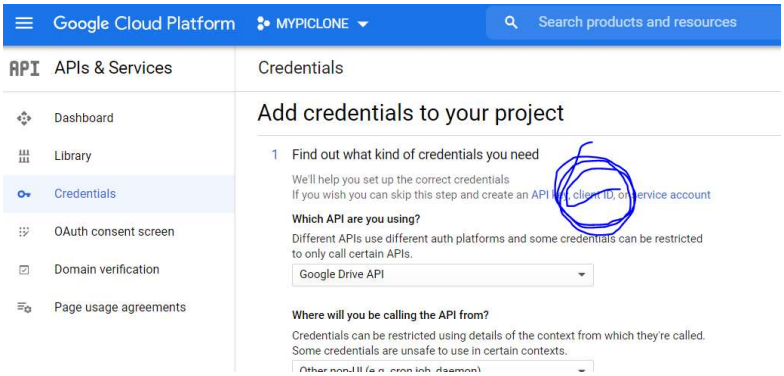
8. Click on **ENABLE**



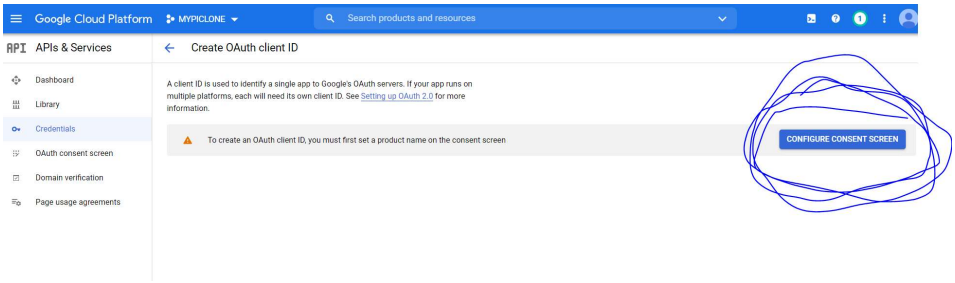
9. Click on **CREATE CREDENTIALS**



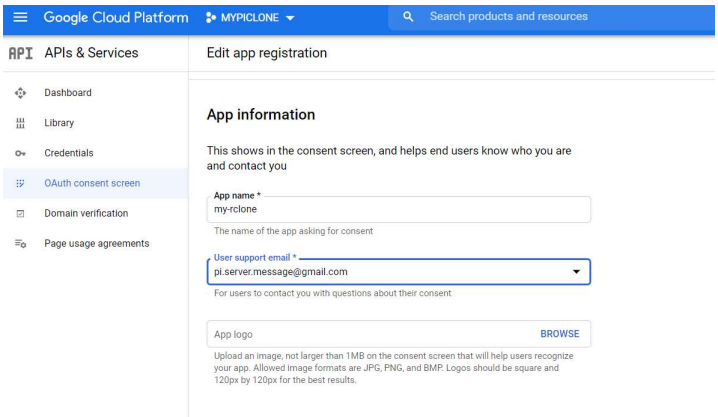
10. Click on **Client ID** (Note: Ignore the other settings here)


Google Cloud Platform
MYPICLONE
Search products and resources
APIs & Services
Credentials
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements
Add credentials to your project
1 Find out what kind of credentials you need
We'll help you set up the correct credentials
If you wish you can skip this step and create an API key, client ID, or service account
Which API are you using?
Different APIs use different auth platforms and some credentials can be restricted to only call certain APIs.
Google Drive API
Where will you be calling the API from?
Credentials can be restricted using details of the context from which they're called.
Some credentials are unsafe to use in certain contexts.

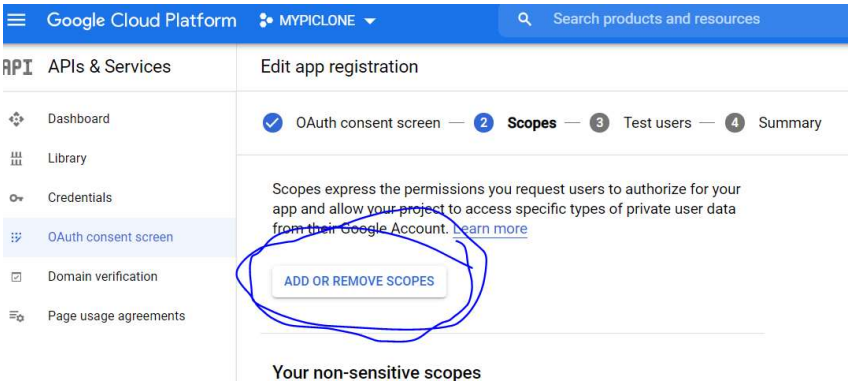
11. Click on **CONFIGURE CONTENT SCREEN**


Google Cloud Platform
MYPICLONE
Search products and resources
APIs & Services
Create OAuth client ID
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements
A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See Setting up OAuth 2.0 for more information.
To create an OAuth client ID, you must first set a product name on the consent screen
CONFIGURE CONSENT SCREEN

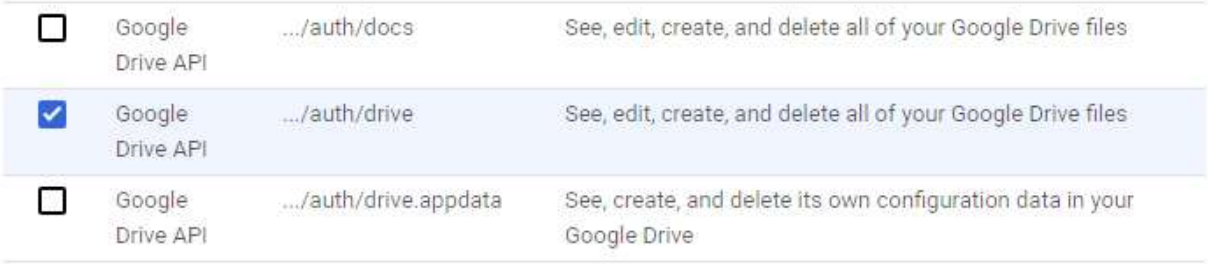
12. Enter your **APP NAME** and **Email**


Google Cloud Platform
MYPICLONE
Search products and resources
APIs & Services
Edit app registration
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements
App information
This shows in the consent screen, and helps end users know who you are and contact you
App name *
my-rclone
The name of the app asking for consent
User support email *
pi.server.message@gmail.com
For users to contact you with questions about their consent
App logo
BROWSE
Upload an image, not larger than 1MB on the consent screen that will help users recognize your app. Allowed image formats are JPG, PNG, and BMP. Logos should be square and 120px by 120px for the best results.

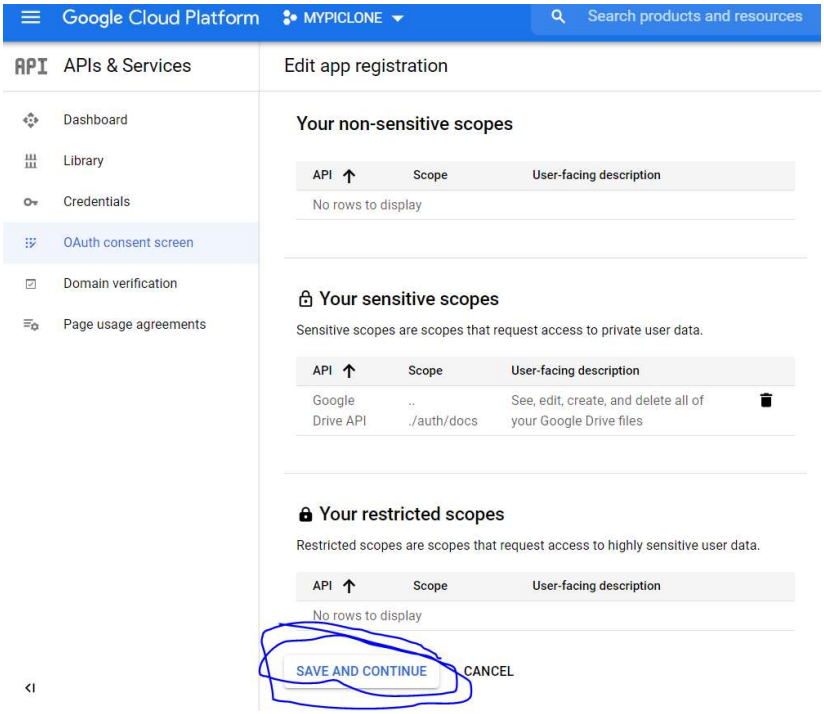
13. Click on **ADD OR REMOVE SCOPE**


Google Cloud Platform
MYPICLONE
Search products and resources
APIs & Services
Edit app registration
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements
OAuth consent screen
2 Scopes
3 Test users
4 Summary
Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. Learn more
ADD OR REMOVE SCOPES
Your non-sensitive scopes

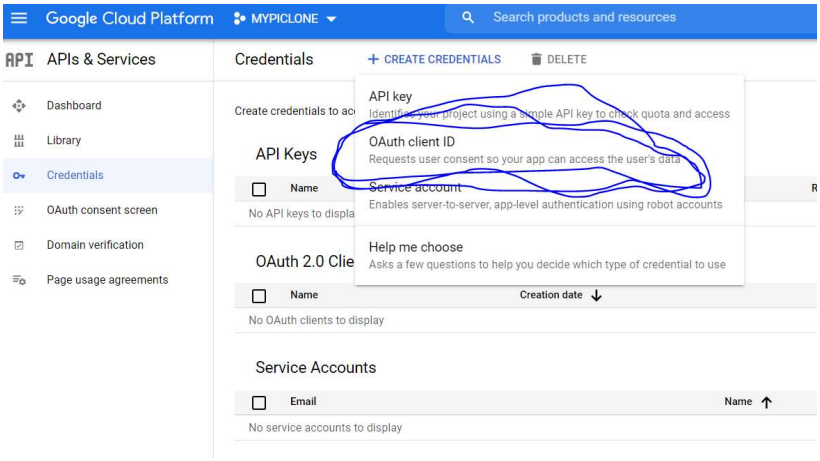
14. Select **GOOGLE DRIVE API** *(SEE, EDIT, CREATE and DELETE GOOGLE DRIVE FILES)* ***AUTH DRIVE***


Google Drive API
.../auth/docs
See, edit, create, and delete all of your Google Drive files
Google Drive API
.../auth/drive
See, edit, create, and delete all of your Google Drive files
Google Drive API
.../auth/drive.appdata
See, create, and delete its own configuration data in your Google Drive

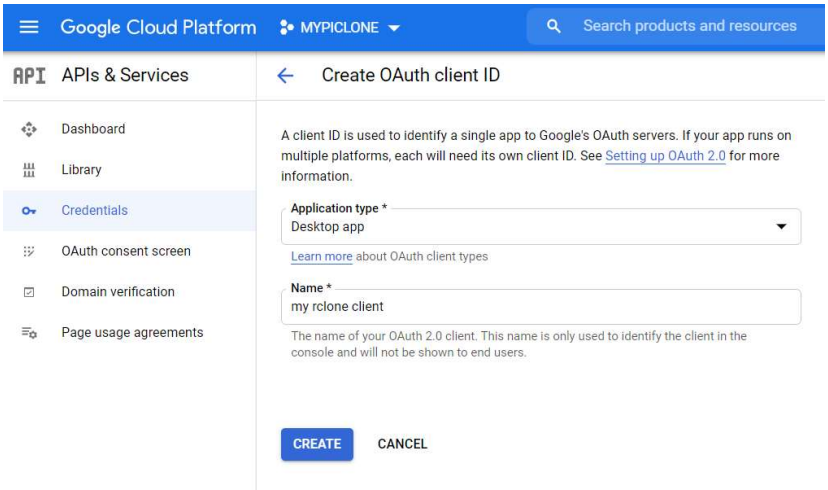
15. Click **SAVE AND CONTINUE**



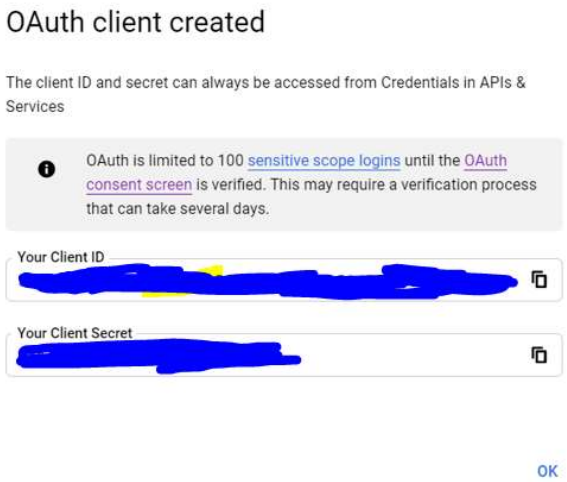
16. Click on **CREDENTIAL** and click on **CREATE CREDENTIALS** and select **OAuth client ID**



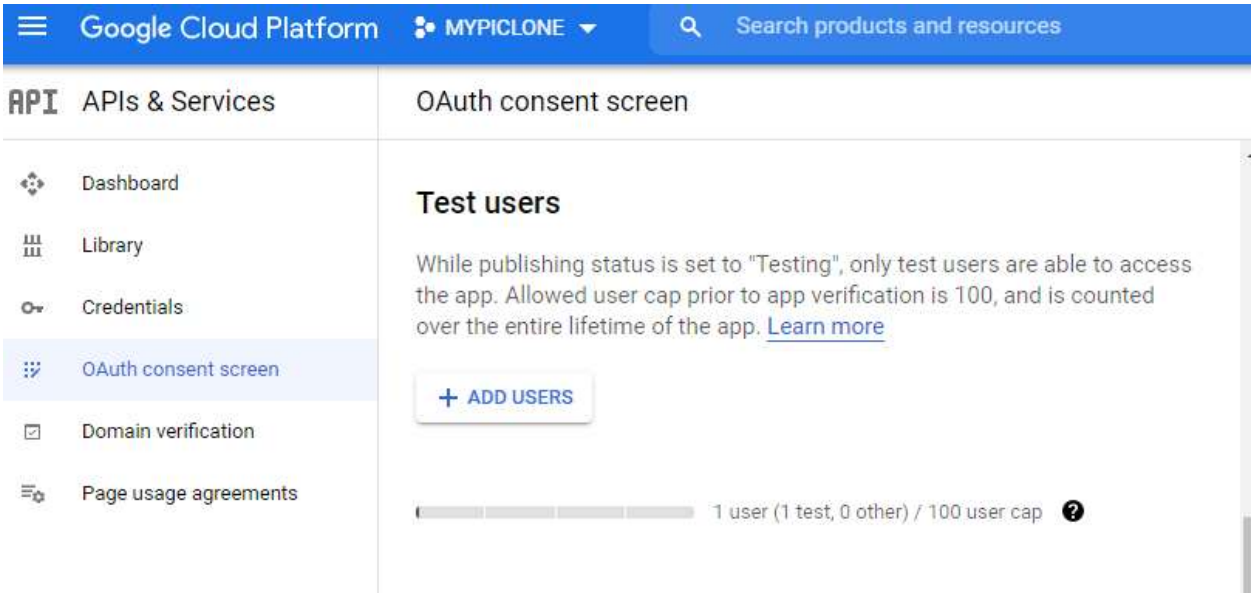
17. Select **DESKTOP APP** under Application Type and under **NAME** enter a name and click **CREATE**


Google Cloud Platform
MYPICLONE
Search products and resources
APIs & Services
Create OAuth client ID
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements
A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See Setting up OAuth 2.0 for more information.
Application type *
Desktop app
Learn more about OAuth client types
Name *
my rclone client
The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.
CREATE
CANCEL

18. You now will be presented with your **Client ID** and **Secret**.


OAuth client created
The client ID and secret can always be accessed from Credentials in APIs & Services
OAuth is limited to 100 sensitive scope logins until the OAuth consent screen is verified. This may require a verification process that can take several days.
Your Client ID
Your Client Secret
OK

19. **Create a test user**, Enter your email for this Gmail account.


Google Cloud Platform
MYPICLONE
Search products and resources
APIs & Services
OAuth consent screen
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements
Test users
While publishing status is set to "Testing", only test users are able to access the app. Allowed user cap prior to app verification is 100, and is counted over the entire lifetime of the app. Learn more
ADD USERS
1 user (1 test, 0 other) / 100 user cap

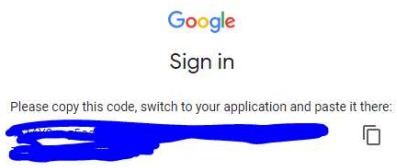
20. **Run RCLONE config** and enter as follows when prompted at each section

```
sudo rclone config
```

```
No remotes found - make a new one
n) New remote
s) Set configuration password
q) Quit config
n/s/q> n

name> gdrive

You will be presented with a list of service select 12 for GDRIVE
Storage> 12

These are examples do not use. Use your own create one.
client_id> 425159802070-
tup27t8cv4h2z3cjkqfmft4n8gjy76lf.apps.googleusercontent.com

These are examples do not use. Use your own created one.
client_secret> MspFTowlsu0SUSRm-1RvcTyx

You will be presented with a list of option select 1 for full access
scope> 1

root_folder_id> Leave Blank empty

service_account_file> Leave Blank empty
```

```
Edit advanced config? (y/n)
y) Yes
n) No
y/n> n

Remote config
Use auto config?
* Say Y if not sure
* Say N if you are working on a remote or headless machine
y) Yes
n) No
y/n> n

These are examples do not use.Open the link in your web browser Copy paste it in.
If your browser doesn't open automatically go to the following link:
https://accounts.google.com/o/oauth2/auth?access_type=offline&client_id=42519807070-tup27t8cv4h2z3cjkqfmfy3n8qju76lf.apps.googleusercontent.com&redirect_uri=urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&response_type=code&scope=https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fdrive&state=1810068827ea077947354c0dab0b80

Log in and authorize rclone for access
```

Open the browser link you were given like above in your web browser. You may be asked login and to allow access twice , until you get the code. Record it in a safe place and enter it as below.




```
These are examples do not use.
Enter verification code>
4/PzWg7ZOEvXIoa9tI7OMjerPq_X5UpsESwwyNvtG8Gf9TK30FERTVrCM

Configure this as a team drive?
y) Yes
n) No
y/n> n
```

```
--------------------
[gdrive]
type = drive
client_id = 4251522066670-
tup27t8cv57husdsftqfmft4n8gju76lf.apps.googleusercontent.com
client_secret = MspFT2feg5SUSRm-1RvcTyx
scope = drive
token =
{"access_token":"xa14.Gv7qcPS5TsadsafpNplGxg5Ndct1gd6yica0d80iFjbKXJ3Kpgn
eZLvn-Tg-YgLPXcEesHubbBcyyeEjGsdd5hg5GhwLnEDxaPhPS3fj6ddTcmMUUOdjOhYW-
rb1xY","token_type":"Bearer","refresh_token":"1/8jxfWbRskdjfd9999ebwK9zfw
ZRHdf43Zhv-9lmtDDC8",
"expiry":"2020-01-23T16:21:03.502362868-07:00"}
--------------------

y) Yes this is OK
e) Edit this remote
d) Delete this remote
y/e/d> y

Current remotes:
Name                 Type
====                 ====
gdrive               drivee) Edit existing remote
n) New remote
d) Delete remote
r) Rename remote
c) Copy remote
s) Set configuration password
q) Quit config
e/n/d/r/c/s/q> q
```

Make the config file accessible so it can be updated by rclone

sudo rclone about gdrive: -vv

```
sudo su
chmod o+rw /root/.config/rclone/rclone.conf
exit
```

21. **Open GDrive** and **create a document** in the root and test if its working

```
sudo rclone ls --max-depth 1 gdrive:
```

```
pi@RaspAP:~ $ rclone ls --max-depth 1 gdrive:
pi@RaspAP:~ $ rclone ls --max-depth 1 gdrive:
       -1 test.docx
pi@RaspAP:~ $
```

WARNING: IF YOU ARE DOING A SYSTEM RESTORE BACKUP AND DOWNLOAD YOUR GDRIVE DATA OR IT COULD BE ALL LOST WHEN SYNC

TESTING (First copy all your data to your share before you sync or copy this is just a test)

```
sudo rclone copy /share gdrive: --fast-list --dry-run
```

COPY DATA (This is the real run, it will erase everything on GDrive and replace it with the USB share)

```
sudo rclone copy /share gdrive: --fast-list
```

22. **Create** the following file

```
sudo nano /home/pi/gsync.sh
```

23. **Enter** the following info into the file

```
#########################################################################
#!/bin/bash
sudo rm /home/pi/mylogfile.txt
sudo rclone sync /share gdrive: --fast-list --log-file=/home/pi/mylogfile.txt
#########################################################################
```

24. When done **Save** and continue

25. Make the file **executable**

```
sudo chmod +x /home/pi/gsync.sh
```

26. Edit the **crontab** to enter a scheduled job once a day (Google restricts daily connection limits)

```
sudo crontab -u pi -e
```

```
################################
0 18 * * * /home/pi/gsync.sh
################################
```

27. **Restart** the **CronTab** service

```
sudo service cron restart
```

Finished

SETUP SERVER HEALTH REPORTS

Resource Guides:
https://linuxhint.com/list-usb-devices-linux/
https://www.pragmaticlinux.com/2020/06/check-the-raspberry-pi-cpu-temperature/
https://www.maketecheasier.com/finding-raspberry-pi-system-information/
https://www.hackster.io/elizabethna/pi-health-dashboard-9935cf

Notes: This is a daily report on the server health
---

1. **Make** and **Admin Directory** in the Samba Share
sudo mkdir /share/Admin

2. **Create** the following file
sudo nano /home/pi/systeminfo.sh

3. **Enter** the following info into the file (Remove the # for email and change for your email)

```
#############################################################################
#!/bin/bash

# DATE INFO
var=$(date +%d-%m-%Y_%H:%M:%S)

# CPU HEAT
var01=$(sudo cat /sys/class/thermal/thermal_zone0/temp)   # Divide by 1000
var00=1000
var0=$((var01 / var00))

# MEMORY USED
var1=$(free -h)

# HDD SPACE ON PI USED IN PERCENT
var2=$(sudo df -h /dev/sda2 | awk '{ SUM += $5} END { print SUM }')

# NETWORK STATUS
var3=$(sudo /sbin/ifconfig)

# CPU INFORMATION
var4=$(sudo cat /proc/cpuinfo)

# RUNNING PROCESSES TREE
var5=$(ps -e --forest)
```

```
# SHOW ALL ACTIVE NETWORK CONNECTIONS
var6=$(sudo netstat -natp)

# SCEDULED TASKS
var7=$(sudo crontab -l -u pi)
var7a=$(sudo crontab -l -u root)

# FSTAB
var8=$(sudo cat /etc/fstab)

# PARTITIONS
var9=$(sudo cat /proc/partitions)

# DISK FREE SPACE USED
sudo du -h / > /share/Admin/DiskUsage.txt

# CONNECTED USB DEVICES
var11=$(lsusb)

# MOUNT INFORMATION
var12=$(mount)

# PING YAHOO TEST
WAITFOR=5
ping yahoo.com -c 4 -i $WAITFOR &> /dev/null
pingReturn=$?

if [ $pingReturn -eq 0 ]; then
# It works
var13="Ping Success!"
#    exit 0
else
# No access
var13="WARNING Ping Failed"
#   exit 1
fi

# OS SYSTEM INFORMATION
var14=$(sudo cat /proc/version)

# AUTH LOGS
sudo cat /var/log/auth.log > /share/Admin/AuthLogs.txt

# SYSTEM MESSAGES
#var16=$(sudo cat /var/log/messages)
# sudo dmesg
sudo cat /var/log/messages > /share/Admin/Messages.txt
```

```
# OUTPUT TO A FILE
printf
"**********************************************************************************
**********\n\nSYSTEM INFORMATION FILE\n$var\n\
n**********************************************************************************
********** \nCPU HEAT\n**********************************\n$var0 Degrees \
n**********************************************************************************
**********\nMEMORY USED\n**********************************\n$var1 \
n**********************************************************************************
**********\nHDD USED\n**********************************\n$var2 Percent \
n**********************************************************************************
**********\nNETWORK STATUS\n**********************************\n$var3 \
n**********************************************************************************
**********\nCPU INFORMATION\n**********************************\n$var4 \
n**********************************************************************************
**********\nRUNNING PROCESS TREE\n**********************************\
n$var5 \
n**********************************************************************************
**********\nACTIVE NETWORK CONNECTIONS\
n**********************************\n$var6 \
n**********************************************************************************
**********\nSCEDULED TASKS CRONTAB\n**********************************\n
USER PI \n$var7 \n USER ROOT \n$var7a \
n**********************************************************************************
**********\nFSTAB MOUNTED DRIVES\n**********************************\
n$var8 \
n**********************************************************************************
**********\nPARTITIONS\n**********************************\n$var9 \
n**********************************************************************************
**********\nCONNECTED USB\n**********************************\n$var11 \
n**********************************************************************************
**********\nMOUNT INFORMATION\n**********************************\
n$var12 \
n**********************************************************************************
**********\nPING YAHOO TEST\n**********************************\n$var13 \
n**********************************************************************************
**********\nOS INFORMATION\n**********************************\n$var14 \
n**********************************************************************************
**********\n\n END OF LINE \n\
n**********************************************************************************
**********" > /share/Admin/SystemHealth.txt
```

```
# THIS IS THE EMAIL SECTION – REMOVE THE # TO ACTIVATE AND EDIT EMAIL

if test -f /share/Admin/SystemHealth.txt; then
sudo chmod o+rw /share/Admin/SystemHealth.txt
sudo chown pi /share/Admin/SystemHealth.txt
fi

if test -f /share/Admin/DiskUsage.txt; then
sudo chmod o+rw /share/Admin/DiskUsage.txt
sudo chown pi /share/Admin/DiskUsage.txt
fi

if test -f /share/Admin/AuthLogs.txt; then
sudo chmod o+rw /share/Admin/AuthLogs.txt
sudo chown pi /share/Admin/AuthLogs.txt
fi

if test -f /share/Admin/Messages.txt; then
sudo chmod o+rw /share/Admin/Messages.txt
sudo chown pi /share/Admin/Messages.txt
fi

if test -f /home/pi/sent.lock; then
sudo rm /home/pi/sent.lock
fi

if test -f /home/pi/sent; then
sudo rm /home/pi/sent
fi

# echo "Raspberry Pi System Health Report Attached" | /usr/bin/mutt -a
/share/Admin/SystemHealth.txt -s "RaspAP Health Report" -- recipient@gmail.com
# sleep 10

# echo "Raspberry Pi System Disk Usage Attached" | /usr/bin/mutt -a /share/Admin/DiskUsage.txt -s
"RaspAP Disc Usage Report" -- recipient@gmail.com
# sleep 10

# echo "Raspberry Pi System Auth logs Attached" | /usr/bin/mutt -a /share/Admin/AuthLogs.txt -s
"RaspAP Auth Report" -- recipient@gmail.com
# sleep10

# echo "Raspberry Pi System Message Logs Attached" | /usr/bin/mutt -a /share/Admin/Messages.txt -s
"RaspAP Message Logs" -- recipient@gmail.com
# sleep 10


if test -f /home/pi/mylogfile.txt; then
```

```
sudo chmod o+rw /home/pi/mylogfile.txt
sudo chown pi /home/pi/mylogfile.txt
fi

#Sleep 10
# echo "GDrive Backup Sync RaspAP Logs " | /usr/bin/mutt -s "GDrive Backup Sync RaspAP Logs" -a
/home/pi/mylogfile.txt -- recipient@gmail.com

#############################################################################
```

4. When done **Save** and continue

5. Make the file **executable**

```
sudo chmod +x /home/pi/systeminfo.sh
```

6. Edit the **crontab** to enter a scheduled job
We create this check **every morning**

```
sudo crontab -u pi -e
```

7. **Enter** the following at the bottom

```
################################
30 7 * * * /home/pi/systeminfo.sh
################################
```

8. When done **Save** and continue

9. **Restart** the **CronTab** service

```
sudo service cron restart
```

Finished

SETUP OVER HEATING ALERTS

Resource Guides:

https://www.raspberrypi.org/documentation/raspbian/applications/vcgencmd.md
Note use vcgencmd command if using a real pi to get the health status of a pie
vcgencmd

Notes:
Pi Systems can sometimes over heat. Checks every 30 minutes
---

1. **Create** the following file
sudo nano /home/pi/heatalert.sh

2. Remove the Hash # to activate email and **enter** the following

```
#############################################################################
#!/bin/bash
# DATE INFO
var=$(date +%d-%m-%Y_%H:%M:%S)

# CPU HEAT
var01=$(sudo cat /sys/class/thermal/thermal_zone0/temp)   # Divide by 1000
var00=1000
var0=$((var01 / var00))
var1=85 # ALERT IF OVER THIS AMOUNT # CHANGE THIS SETTING FOR MAX TEMP TO MONIT$

# REMOVE THE HASH TO DELETE THE HEAT FILE AUTOMATICLY
if (($var0 < $var1))
then
if test -f /share/EMERCENCY-HEAT-ALERT-CALL-ADMIN.txt; then
##sudo rm /share/EMERCENCY-HEAT-ALERT-CALL-ADMIN.txt
fi
fi

if (($var0 > $var1))
then
printf "*****************************\n\nCPU HEATING ALERT\n$var\n\
n***************************** \nCPU HEAT\n\n$var0 Degrees \
n*****************************" > /share/EMERCENCY-HEAT-ALERT-CALL-ADMIN.txt
sudo chown pi /share/EMERCENCY-HEAT-ALERT-CALL-ADMIN.txt
#############################################################################
# THIS IS THE EMAIL SECTION REMOVE HASH SIGN TO ACTIVATE
```

```
echo -e "Subject: Overheating RaspAP Alert\r\n\r\nRaspberry Pi Server RaspAP is overheating with $var0 Degrees" | msmtp --debug --from=default -t youremailaddress@gmail.com
fi
################################################################################
```

3. Make the file **executable**

```
sudo chmod +x /home/pi/heatalert.sh
```

4. **Enter the crontab** to enter the scheduled job for checking
We create a check every 30 minutes

```
sudo crontab -u pi -e
```

5. **Enter** the following at the bottom of the file

```
################################
*/30 * * * * /home/pi/heatalert.sh
################################
```

6. **Save** the settings when done

7. **Restart** the **CronTab** service

```
sudo service cron restart
```

Finished

SETUP SYSTEM LOW DISC SPACE ALERTS

Resource Guides:
https://stackoverflow.com/questions/27491881/linux-command-to-lookup-total-disk-and-harddrive-numbers

Notes:
The USB or HDD can get full and stop everything working (We can make the computer beep)
---

1. **Create** the following file
sudo nano /home/pi/drivewarn.sh

2. **Enter** the following into the file

```
##############################################################################

#!/bin/bash
# SHOW THE PERCENT USED OF PARTITION
var1="sudo df -h /dev/sda2 | awk '{ SUM += $5} END { print SUM }'" # The sum is in % used
var2=90 # THE AMOUNT SPACE USED TO TRIGGER THE ALERT SET TO 90% OF DRIVE

if (($var1 > $var2))
then
printf "DRIVE SDA2 IS FULL\n \n---------- \nSPACE USED = $var1 Percent \n----------\nSPACE LIMIT = $var2 Percent \n----------\n \nPLEASE REDUCE FILES" > /share/EMERCENCY-HDD-FULL-CALL-ADMIN.txt
##############################################################################
# THIS IS THE EMAIL SECTION REMOVE HASH SIGN TO ACTIVATE
# echo -e "Subject: Server Drive Full Alert\r\n\r\nRaspberry Pi Server RaspAP is Full with $var1 Percent of Drive Used" | msmtp --debug --from=default -t recipient@gmail.com
##############################################################################
fi

if (($var1 < $var2))
then
FILE=/share/EMERCENCY-HDD-FULL-CALL-ADMIN.txt
if test -f "$FILE"; then
sudo rm /share/EMERCENCY-HDD-FULL-CALL-ADMIN.txt
fi
fi
```

```
# REMOVE THE HASH AT ECHO AND SLEEP TO ACTIVATE PC SOUND
if (($var1 > $var2))
then
# MAKE SOME BEEP IF DRIVE GETTING FULL
##echo -en "\007"
##sleep 2
##echo -en "\007"
##sleep 2
##echo -en "\007"
##sleep 2
##echo -en "\007"
##sleep 2
##echo -en "\007"
fi

#############################################################################
```

3. **Save** your file when done

4. Make the file **executable**

```
sudo chmod +x /home/pi/drivewarn.sh
```

5. **Enter** into the **crontab** the **scheduled job**
We create this check every hour

```
sudo crontab -u pi -e
```

```
##################################
*/45 * * * * /home/pi/drivewarn.sh
##################################
```

6. Save your file when done

7. **Restart** the **CronTab** service

```
sudo service cron restart
```

Finished

SETUP CLAM ANTI-VIRUS SCANNING AND ALERTS

Resource Guides:
https://pimylifeup.com/raspberry-pi-clamav/

Notes: Since we have a shared unsecured folder we need to scan the system and folders for threats daily
WARNING: SCANNING ON A USB CAN GREATLY EFFECT THE SPEED OF THE SYSTEM
clamscan -r /home /mount
clamscan -r --move=/quarantine/ /home
clamscan -r --remove /home /mount
---

1. **Create** the directory for the log reports
sudo mkdir -m 1777 /var/log/clamav/

2. **Create** the quarantine directory to move infected files into
sudo mkdir -m 1777 /quarantine

3. Install CLAMAV and when prompted select **y** for **yes**
sudo apt install clamav

4. **Create** the script file
sudo nano /home/pi/scanvirus.sh

5. **Enter** the following in to the file and remove the hash and change the email to email the scan logs

```
#########################################################
#!/bin/bash
# REMOVE THE OLD LOG FILE SO WE DON'T BUILD A LARGE FILE WITH OLD DATA
sudo rm /var/log/clamav/clamavreport.log

# UPDATE THE CLAM DATABASE (WE NEED TO STOP THE SERVICE DUE TO AN ERROR)
sudo /etc/init.d/clamav-freshclam stop
sudo freshclam
sudo /etc/init.d/clamav-freshclam start

sudo timeout 2h clamscan -r -i /share --move=/quarantine/ --log=/var/log/clamav/clamavreport.log

#############################################################################
# THIS IS THE EMAIL SECTION – REMOVE THE # TO ACTIVATE AND EDIT EMAIL
if test -f /var/log/clamav/clamavreport.log; then
sudo chmod o+rw /var/log/clamav/clamavreport.log
fi
```

```
if test -f /home/pi/sent.lock; then
sudo rm /home/pi/sent.lock
fi

if test -f /home/pi/sent; then
sudo rm /home/pi/sent
fi

echo "Clam Anti-Virus Report Log Attached" | /usr/bin/mutt -a /var/log/clamav/clamavreport.log -s
"RaspAP Clam Anti-Virus Report" -- recipient@gmail.com
################################################################################
```

6. When done editing, **save** your file

7. Make the file **executable**

```
sudo chmod +x /home/pi/scanvirus.sh
```

8. **Enter** into the **crontab** the **scheduled job**
We create this check every hour

```
sudo crontab -u pi -e
```

```
################################
0 22 * * * /home/pi/scanvirus.sh
################################
```

9. **Save** your file when done

10. **Restart** the **CronTab** service

```
sudo service cron restart
```

11. **Reboot** the **computer**

```
sudo reboot
```

Finished

CCTV Monitor (Raspberry WebCam Monitoring)

Resource Guides:
https://wolfpaulus.com/raspberrypi_webcam/
https://www.instructables.com/How-to-Make-Raspberry-Pi-Webcam-Server-and-Stream-/
https://pimylifeup.com/raspberry-pi-webcam-server/
https://linuxhint.com/list-usb-devices-linux/
https://motion-project.github.io/motion_build.html
https://electronnicproject.blogspot.com/2017/07/raspberry-pi-surveillance-camera-with.html

Notes: sudo service motion restart
sudo service motion stop
lsusb
dmesg | less
usb-devices
---

1. Run the **Update**
sudo apt-get update

2. **Install** all the dependencies
sudo apt install autoconf automake build-essential pkgconf libtool git libzip-dev libjpeg-dev gettext libmicrohttpd-dev libavformat-dev libavcodec-dev libavutil-dev libswscale-dev libavdevice-dev default-libmysqlclient-dev libpq-dev libsqlite3-dev libwebp-dev

3. Download Motion and **install**
sudo apt-get install motion

4. **Edit** the **config** file and change as below
sudo nano /etc/motion/motion.conf

##########################

daemon on

Set none or v or h for camera flipping or none
flip_axis v

width 640

height 480

framerate 100

output_pictures best

ffmpeg_output_movies off #(Change this option to **on** if you want videos recorded)

stream_maxrate 100

stream_localhost off

pre_capture 1

post_capture 1

Here you can set timed shots in seconds
snapshot_interval 0

DEPENDING ON YOUR VERSION CHOOSE THE ONE RELEVANT TO YOU
ffmpeg_timelapse 2
timelapse_interval 2

target_dir /share/motion

max_movie_time 20

threshold 1500

minimum_motion_frames 5

logfile /var/logs/motion/motion.log

auto_brightness on

stream_auth_method 1

; stream_authentication pi:raspberry

CHANGE THE FILE FORMAT SO EMAILING WILL WORK FROM
#picture_filename %v-%Y%m%d%H%M%S-%q
picture_filename capture

CHANGE THE FILE FORMAT SO EMAILING WILL WORK FROM
#movie_filename %v-%Y%m%d%H%M%S
movie_filename cctvfilm

CHANGE THE FILE FORMAT SO EMAILING WILL WORK FROM
#timelapse_filename %Y%m%d-timelapse
timelapse_filename timelapse

############################

6. **Save** the settings

7. **Change** the following

```
sudo nano /etc/default/motion
```

```
##########################
start_motion_daemon=yes
##########################
```

8. **Save** settings

9. Make the following **directories**

```
sudo mkdir -m 1777 /share/motion
```

```
sudo mkdir -m 1777 /share/motion/archive
```

10. **Start the Service**

```
sudo service motion restart
```

11. **Open** your **web Browser** and view

```
http://192.168.0.2:8081
```

12. **Check** the **folder** for recording or Images

```
ls -al  //share/motion
```

13. Let's **create** an **email** alert with endless looping

```
sudo touch /home/pi/CCTVStart.sh
```

14. **Change permissions** to be executed

```
sudo chmod +x /home/pi/CCTVStart.sh
```

15. **Edit** the file

```
sudo nano /home/pi/CCTVStart.sh
```

```
####################################
#!/bin/bash
if test -f /home/pi/sent.lock; then
sudo rm /home/pi/sent.lock
fi
if test -f /home/pi/sent; then
sudo rm /home/pi/sent
fi
if test -f /share/motion/timelaps.mpg; then
sudo rm /share/motion/timelaps.mpg
fi
if test -f /share/motion/capture.jpg; then
sudo rm /share/motion/capture.jpg
fi
```

```
if test -f /share/motion/cctvfilm.mkv; then
sudo rm /share/motion/cctvfilm.mkv
fi

sudo service motion start

while true
do

# IF YOU WISH TO SEND CAPTURED FILMS AND YOU ENABLED IT ABOVE REMOVE THE #
#if test -f /share/motion/cctvfilm.mkv; then
#echo "Check the attachments for CCTV activity or login at http//192.168.0.2:8081" | /usr/bin/mutt -a
/share/motion/cctvfilm.mkv -s "CCTV ACTIVITY" -- youremailaddress@gmail.com
#sleep 5
# REMOVE THE # TO DELETE OR MOVE TO ARCHIVE NOTE COULD FILL THE DRIVE QUICK
## sudo mv /share/motion/cctvfilm.mkv /share/motion/archive/
#sudo rm /share/motion/cctvfilm.mkv
#fi

if test -f /share/motion/capture.jpg; then
echo "Check the attachments for CCTV activity or login at http//192.168.0.2:8081" | /usr/bin/mutt -a
/share/motion/capture.jpg -s "CCTV ACTIVITY" -- youremailaddress@gmail.com
sleep 5
# REMOVE THE # TO DELETE OR MOVE TO ARCHIVE NOTE COULD FILL THE DRIVE QUICK
# sudo mv /share/motion/capture.jpg /share/motion/archive/
sudo rm /share/motion/capture.jpg
fi

done
#####################################
```

16. **Save** the settings

17. **RUN THE MOTION CAMERA AT NIGHT AT HOME for 6 Hours (You decide)**

```
sudo crontab -u pi -e

#################################
0 1 * * timeout 5h /home/pi/CCTVStart.sh
0 6 * * * sudo service motion stop
@reboot sudo service motion stop
#################################
```

18. **Restart** the **CronTab** service

```
sudo service cron restart
```

Finished

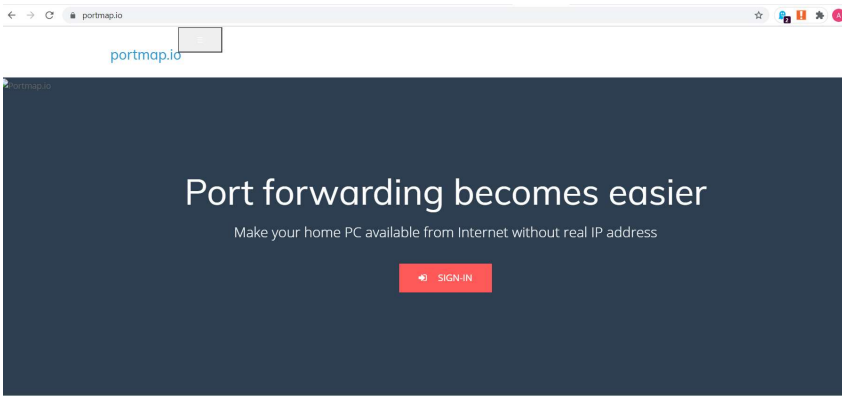
PORT FORWARDING TO SEE THE CCTV CAMERA FROM THE INTERNET (NO ROUTERS NEEDED)

Resource Guides:
http://www.portmap.io

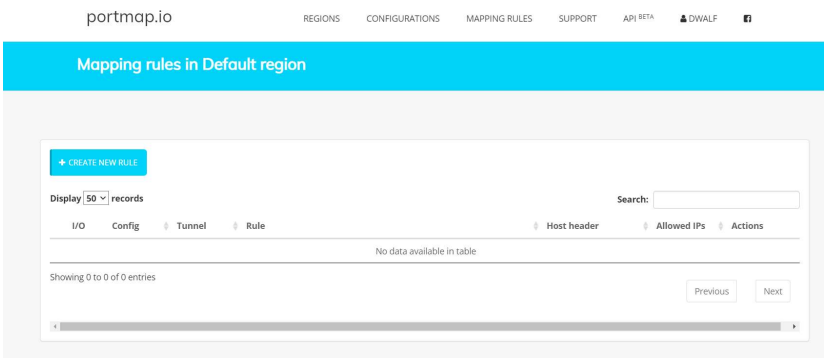
Notes: This will allow you to see your CCTV regardless of been blocked by your ISP or sitting behind a private network on your router. If you have a static internet IP you can port forward from the router without the other steps. (Many documents on the internet how to do this)

systemctl start openvpn # Starts OpenVPN and connects to OVPN
systemctl stop openvpn # Stops OpenVPN
systemctl restart openvpn # Restarts OpenVPN
systemctl status openvpn # Shows status for OpenVPN

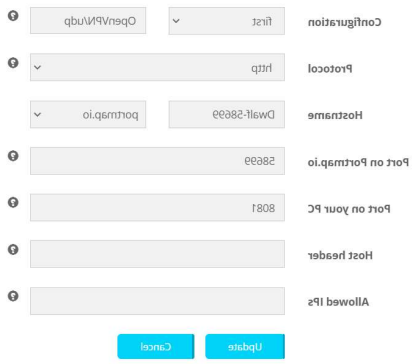
1.**Login** or **register** an account for free at http://www.portmap.io



2.Click on **CREATE A NEW RULE**

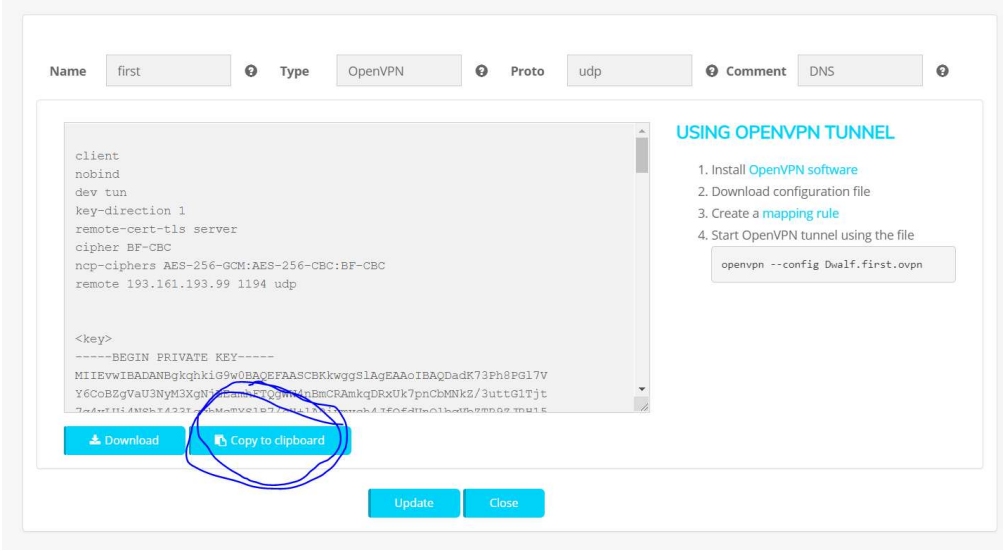


3.Set the new rule with **HTTP** and the **PORT ON PC** to **8081** for the CCTV Monitor Webpage.

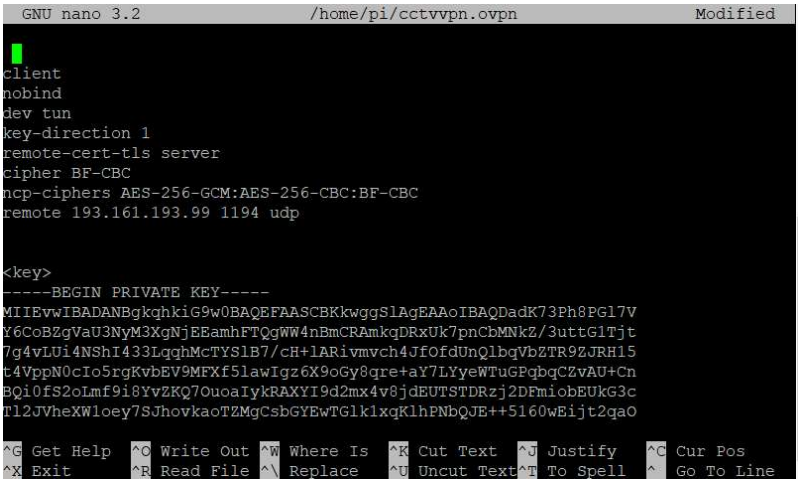


4.Click on **FIRST** to reveal the connection data.

5.Click on **COPY TO CLIPBOARD**



6.**Create** the file **cctvvpn.ovpn** and **paste** the data by right clicking from the **clipboard from portmap.io**
sudo nano /home/pi/cctvvpn.ovpn



7.**Save** the file

8.**Install** the openvpn software (reboot after the install if needed and enter y if prompted during install)
sudo apt-get install openvpn

9.**Setup the openvpn start service** to connect to the VPN by creating a script file
sudo nano /home/pi/remotecctvstart.sh

```
#####################################
#!/bin/bash
sudo openvpn --config /home/pi/cctvvpn.ovpn --daemon
#####################################
```

10.**Save** your settings

11.Change permissions to be executed
sudo chmod +x /home/pi/remotecctvstart.sh

12.**Setup the openvpn disconnect service** to end the VPN by creating a script file
sudo nano /home/pi/remotecctvend.sh

```
#####################################
#!/bin/bash
sudo killall openvpn
#####################################
```

12.**Save** your settings

13.Change permissions to be executed
sudo chmod +x /home/pi/remotecctvend.sh

14.**Setup the crontab** to run the service when the REMOTE CCTV VPN is to be switch on
`sudo crontab -u pi -e`

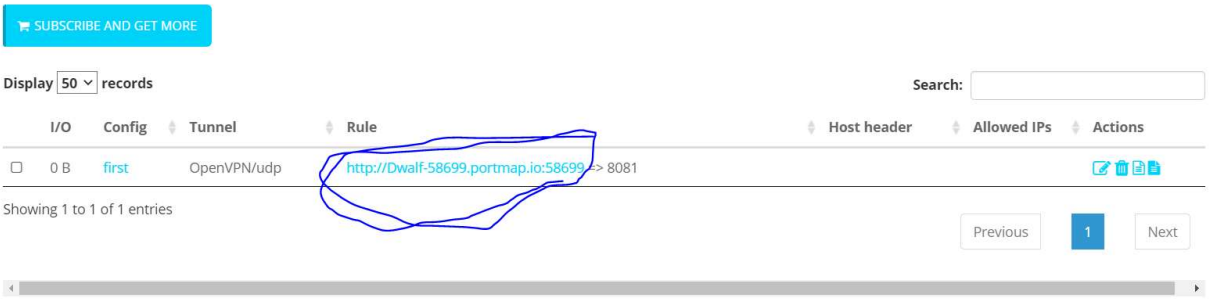
15.**Enter** the following

```
################################
58 0 * * * /home/pi/remotecctvstart.sh
5 6 * * * /home/pi/remotecctvend.sh
################################
```

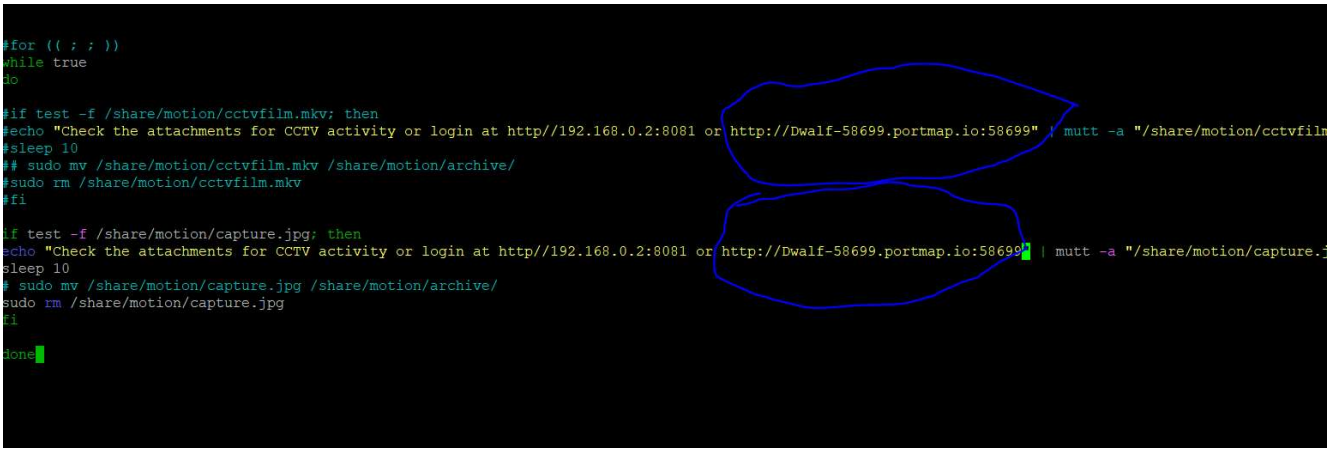
16.**Save** the settings

17. **Restart** the **CronTab** service
`sudo service cron restart`

18.Go back **to portmap.io** and get the **rule address (Write it down)**



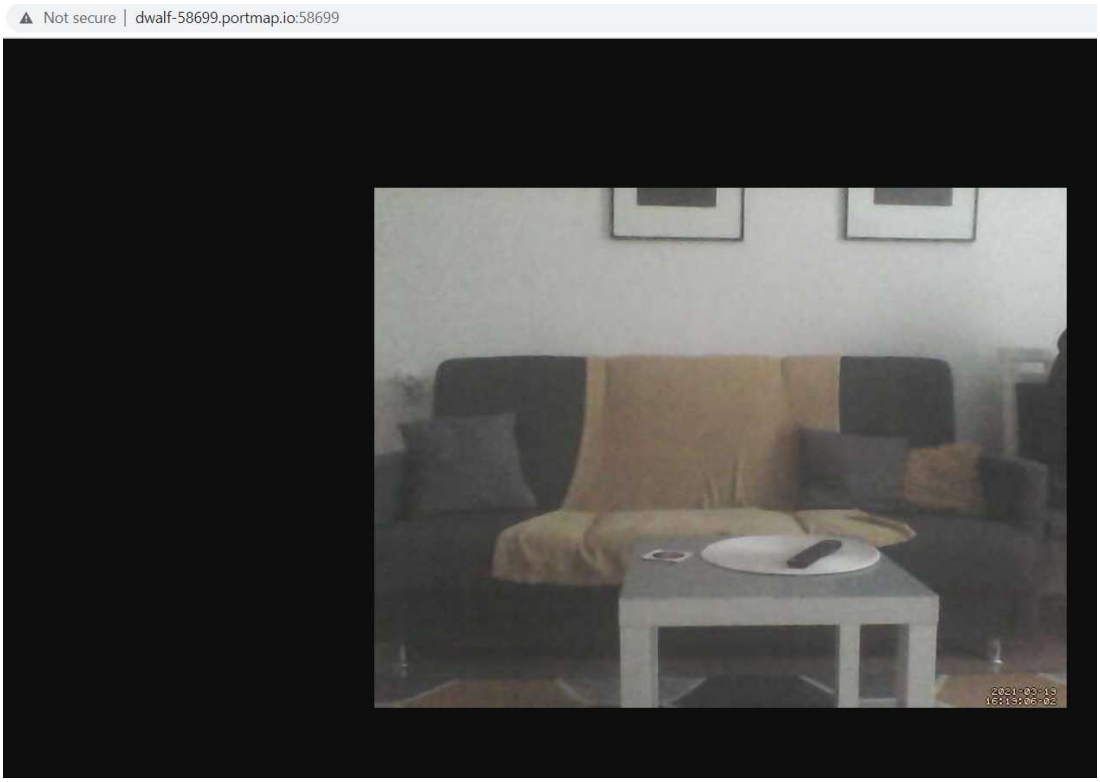
19.Lets **edit the email** from the CCTV Motion Setup to reflect the **outside URL address**
Get ready with the URL and port portmap.io give you.
Example: http://Dwalf-58669.portmap.io:58699
`sudo nano /home/pi/CCTVStart.sh`


#for ((; ;))
while true
do
#if test -f /share/motion/cctvfilm.mkv; then
#echo "Check the attachments for CCTV activity or login at http//192.168.0.2:8081 or http://Dwalf-58699.portmap.io:58699" | mutt -a "/share/motion/cctvfilm
#sleep 10
sudo mv /share/motion/cctvfilm.mkv /share/motion/archive/
#sudo rm /share/motion/cctvfilm.mkv
#fi
if test -f /share/motion/capture.jpg; then
echo "Check the attachments for CCTV activity or login at http//192.168.0.2:8081 or http://Dwalf-58699.portmap.io:58699" | mutt -a "/share/motion/capture.
sleep 10
# sudo mv /share/motion/capture.jpg /share/motion/archive/
sudo rm /share/motion/capture.jpg
fi
done

20.When finished editing **save**

21. **Test** your external link from a **mobile phone internet**. Open your link from portmap.io
sudo systemctl start openvpn
sudo service motion start
/home/pi/remotecctvstart.sh

Example Link: http://Dwalf-58699.portmap.io:58699



22. When finished **testing, stop** the service if need be.
sudo service motion stop

/home/pi/remotecctvend.sh

23.Make sure your motion **config file is setup to authenticate with a username and password**. You should be prompted for one if you followed this guide. **pi/raspberry**

Finished

WARNING:

BEFORE YOU CONTINUE
SELECT ONLY ONE OF THE FOLLOWING SETUPS

OPTION 1:

RASPAP
SETUP WIFI ON AND OFF

OPTION 2:

PI-HOLE
SETUP PI WEBSERVER FOR EASY ACCESS
UNBOUND

YOU CANNOT SELECT BOTH OPTIONS AS THIS WILL CORRUPT YOUR INSTALATION. ANOTHER OPTION WOULD BE TO INSTALL ON A DIFFERENT SYSTEM

RaspAP - Raspberry Wireless Access Point

Resources Guides:
https://raspap.com/

Notes: This is OPTIONAL, YOU CAN USE YOUR ROUTER WIFI, ALSO THERE IS SOME BUGGY BITS WITH THE STATIC IP ON THE LAN – HENCE THE NEED FOR A DHCP RESERVATION ON YOUR ROUTER, I NOTICED SOME WIFI USB IS NOT AS GOOD IN STREANTH AS A DEFAULT ROUTER WIFI AP. I AM USING A USB WIFI (**Ralink Technology, Corp. RT5370**) I have also tested with other cheap WIFI USB did not work at all)

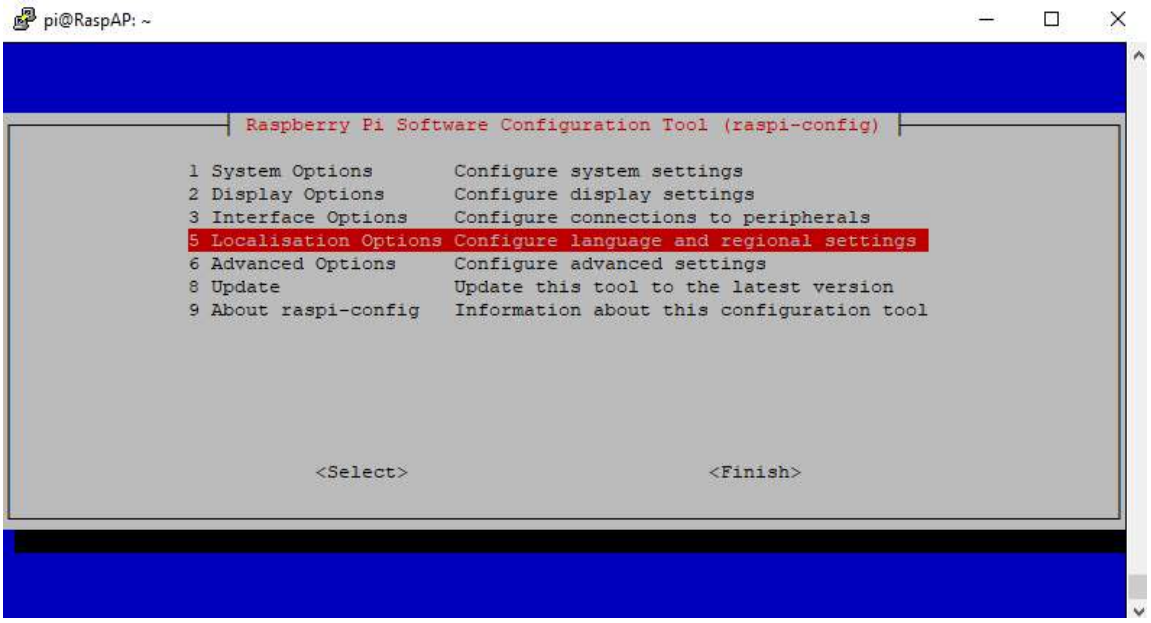
---

1. First **update**
   sudo apt-get update

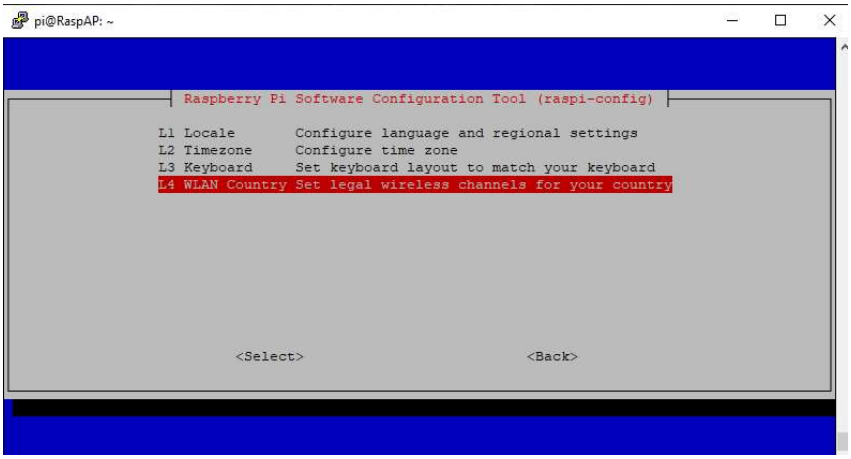
2. After the update **reboot**
   sudo reboot

3. IMPORTANT: We need to **set the localization** of the **WIFI** else the setup will fail.
   sudo raspi-config

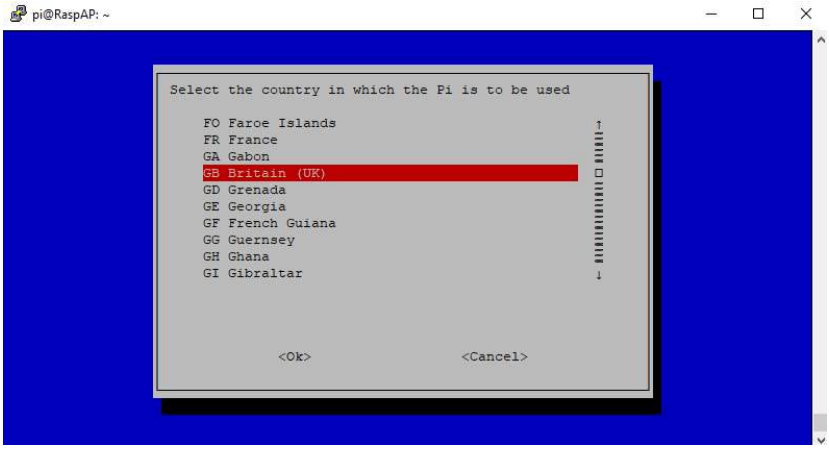
4. Select **5 Localization Options** Menu


pi@RaspAP: ~
Raspberry Pi Software Configuration Tool (raspi-config)
1 System Options Configure system settings
2 Display Options Configure display settings
3 Interface Options Configure connections to peripherals
5 Localisation Options Configure language and regional settings
6 Advanced Options Configure advanced settings
8 Update Update this tool to the latest version
9 About raspi-config Information about this configuration tool
<Select>
<Finish>

5. Select **L4 WLAN Country Set Legal wireless channels** for your country


pi@RaspAP: ~
Raspberry Pi Software Configuration Tool (raspi-config)
L1 Locale Configure language and regional settings
L2 Timezone Configure time zone
L3 Keyboard Set keyboard layout to match your keyboard
L4 WLAN Country Set legal wireless channels for your country
<Select>
<Back>

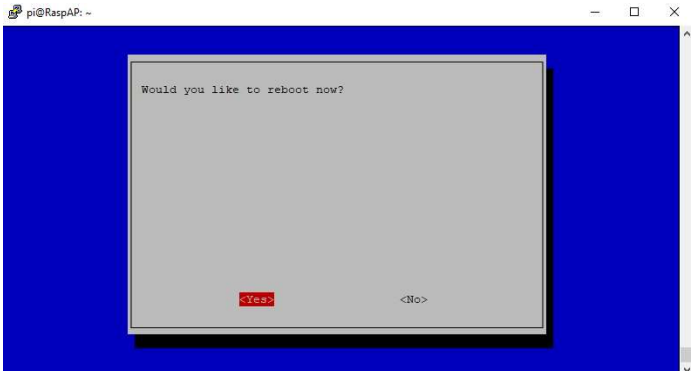
6. Select your country (example **GB**)



7. Select **OK**

8. **Tab** select **FINISH**

9. You will be asked to **reboot**.
   Tab Select **YES**

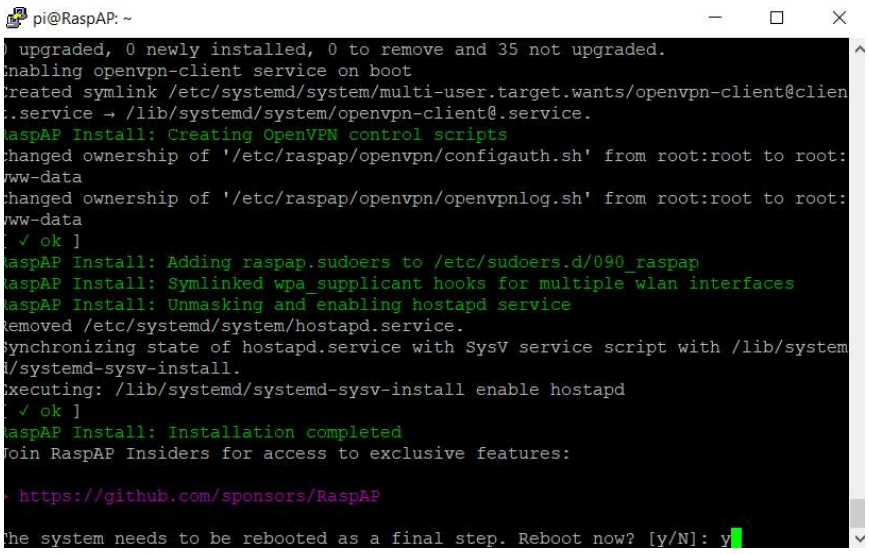


10. The system will **reboot.**

11. Next we **run** the script for **RaspAP** (Raspberry Access Point) Installer
    While the quick installer runs select **Y** (yes) for all options

    ```
    curl -sL https://install.raspap.com | bash
    ```

12. **When Finished Installing Reboot** the system, select **Y** to reboot.


pi@RaspAP: ~
upgraded, 0 newly installed, 0 to remove and 35 not upgraded.
nabling openvpn-client service on boot
reated symlink /etc/systemd/system/multi-user.target.wants/openvpn-client@clien
.service → /lib/systemd/system/openvpn-client@.service.
aspAP Install: Creating OpenVPN control scripts
hanged ownership of '/etc/raspap/openvpn/configauth.sh' from root:root to root:
ww-data
hanged ownership of '/etc/raspap/openvpn/openvpnlog.sh' from root:root to root:
ww-data
[✓ ok]
aspAP Install: Adding raspap.sudoers to /etc/sudoers.d/090_raspap
aspAP Install: Symlinked wpa_supplicant hooks for multiple wlan interfaces
aspAP Install: Unmasking and enabling hostapd service
emoved /etc/systemd/system/hostapd.service.
ynchronizing state of hostapd.service with SysV service script with /lib/system
/systemd-sysv-install.
xecuting: /lib/systemd/systemd-sysv-install enable hostapd
[✓ ok]
aspAP Install: Installation completed
oin RaspAP Insiders for access to exclusive features:
https://github.com/sponsors/RaspAP
he system needs to be rebooted as a final step. Reboot now? [y/N]: y

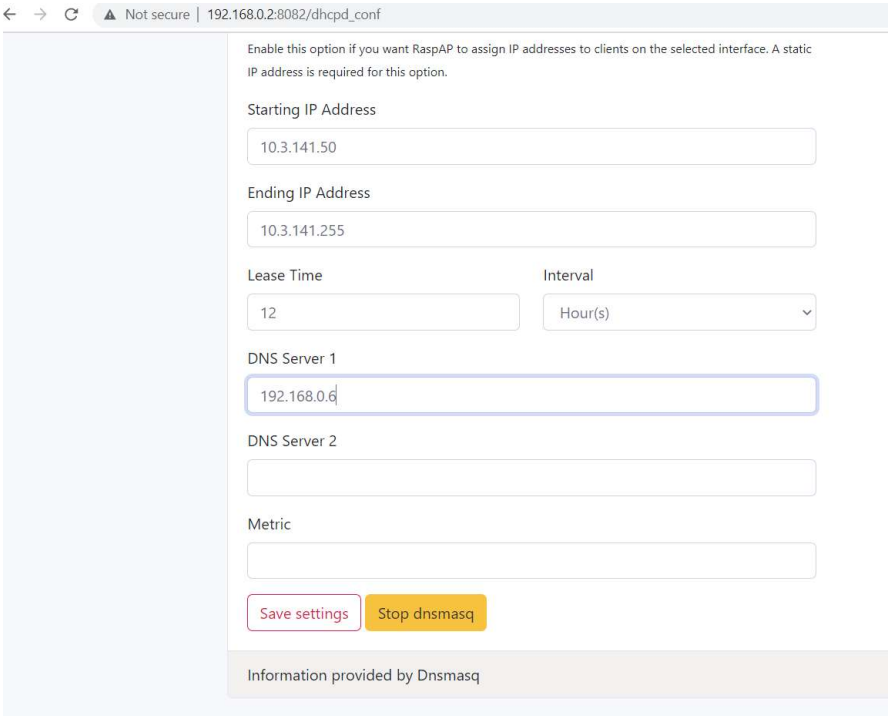
13. You should now have the following setting **defaulted settings**

****
DEFAULT SETUP FOR RASPAP SETTINGS (CAN BE CHANGED IN THE WEB ADMIN PAGE)
****
IP address: 10.3.141.1
Username: admin
Password: secret
DHCP range: 10.3.141.50 to 10.3.141.255
SSID: raspi-webgui
Password: ChangeMe
****

NOTE:
The Setup will change the /etc/dhcpcd.conf file and remove the static address
Its possible to set up the static address in the RaspAP webpage under DHCP and select eth0
Web Admin if on wifi = http://10.3.141.1
Personally I would just set a reservation in your DHPC on your router and not mess with it. It has broken before for me.

14.**If you already have a PI-HOLE setup on another computer** then **DHCP DNS** to point to your **Pi-HOLE**

Example: 192.168.0.6 or leave BLANK
WATCHOUT WITH THESE SETTINGS AS IT HAS A HABBIT OF LOOSING ALL INFO



15.**OPTIONAL:** If you have issues edit and **repair**
sudo nano /etc/dhcpcd.conf

Where static domain name server is you can use **8.8.8.8 8.8.8.4.4** if not using PI-HOLE
MAKE SURE THERE IS NO EMPTY SPACES AFTER THE SETTINGS

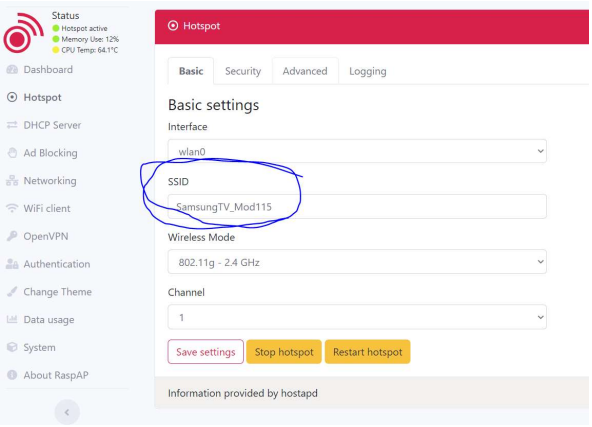
```
# RaspAP default configuration
hostname
clientid
persistent
option rapid_commit
option domain_name_servers, domain_name, domain_search, host_name
option classless_static_routes
option ntp_servers
require dhcp_server_identifier
slaac private
nohook lookup-hostname

# RaspAP wlan0 configuration
interface wlan0
static ip_address=10.3.141.1/24
static routers=10.3.141.1
static domain_name_server=192.168.0.6
```

16. We need to **modify** the **UFW firewall** to serve RaspAP DHCP clients so edit the following
sudo nano /etc/default/ufw

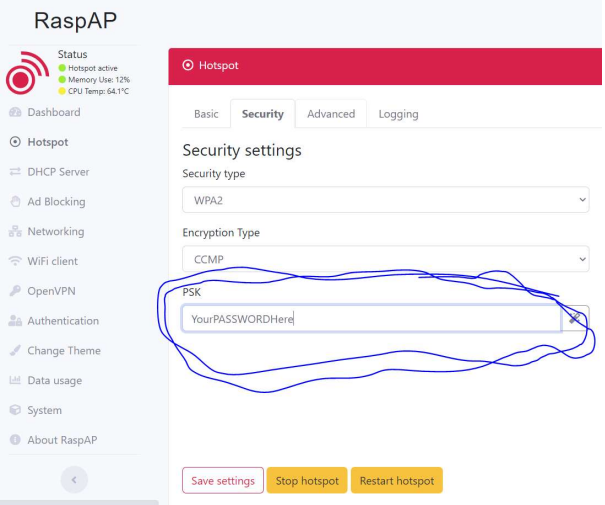
17.Change the following to ACCEPT

```
##################################################################
# Set the default forward policy to ACCEPT, DROP or REJECT.  Please note that
# if you change this you will most likely want to adjust your rules
DEFAULT_FORWARD_POLICY="ACCEPT"
##################################################################
```

18.To change the **Wireless SSID** select **HOTSPOT**, change the SSID and **SAVE SETTINGS**



19.Next Click on **SECURITY** and change the password then **SAVE SETTINGS** and **RESTART HOTSPOT**



Finished

SETUP WIFI ON AND OFF (LESS EMF RADIATION)

Resources Guides:
https://www.raspberrypi.org/documentation/linux/usage/cron.md
https://discussions.flightaware.com/t/how-to-setup-nightly-reboots-for-your-raspberry-pi/15821
https://raspberrytips.com/disable-wifi-raspberry-pi/

Notes:
Less radiation and keeping hackers away at night
To see the date and time type the command
`date`
To see the crontab jobs type the command
`sudo crontab -l`

1.**Create** the following **file**
`sudo nano /home/pi/wifiup.sh`

2.**Enter** the following

```
################################
#!/bin/bash
sudo ifconfig wlan0 up
################################
```

3.**Save** the settings

4.**Make** the file **executable**
`sudo chmod +x /home/pi/wifiup.sh`

5.**Create** the following **file**
`sudo nano /home/pi/wifidown.sh`

6.**Enter** the following

```
################################
#!/bin/bash
sudo ifconfig wlan0 down
################################
```

7.**Save** the settings

8.**Make** the file **executable**
sudo chmod +x /home/pi/wifidown.sh

9.**Enter** the **crontab** to enter the scheduled job
Off at 1am and back on at 6am

sudo crontab -u pi -e

```
################################
0 1 * * * /home/pi/wifidown.sh
0 6 * * * /home/pi/wifiup.sh
################################
```

10.**Save** the settings

11. **Restart** the **CronTab** service
sudo service cron restart

12.**Test** to see if the **WIFI** is up or down enter
sudo ifconfig

Note rebooting the system will activate the wireless again

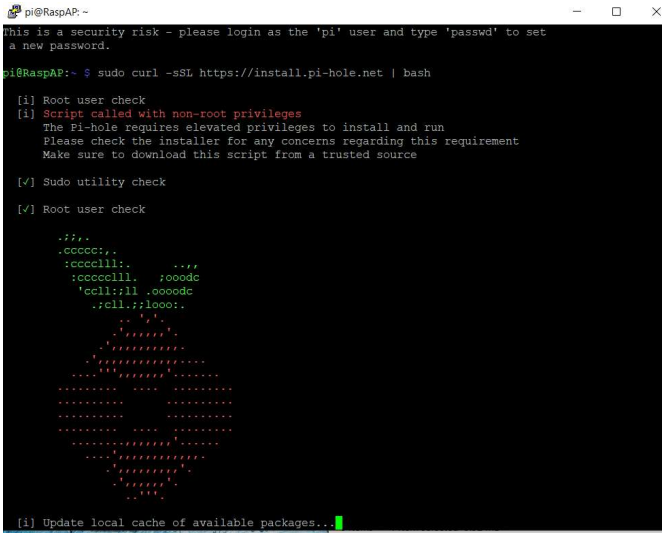
Finished

INSTALLING PI-HOLE (DNS BLACKHOLE)

Resources Guides:
https://docs.pi-hole.net/main/basic-install/
https://www.smarthomebeginner.com/pi-hole-setup-guide/
https://www.smarthomebeginner.com/pi-hole-setup-guide/
https://github.com/mmotti/pihole-regex/blob/master/regex.list
https://lunarwatcher.github.io/posts/2020/05/17/what-i-learned-after-using-pihole-for-a-week.html
https://planeteggroll.home.blog/2019/01/27/pi-hole-installation-and-tweaks/
https://discourse.pi-hole.net/t/why-should-pi-hole-be-my-only-dns-server/3376

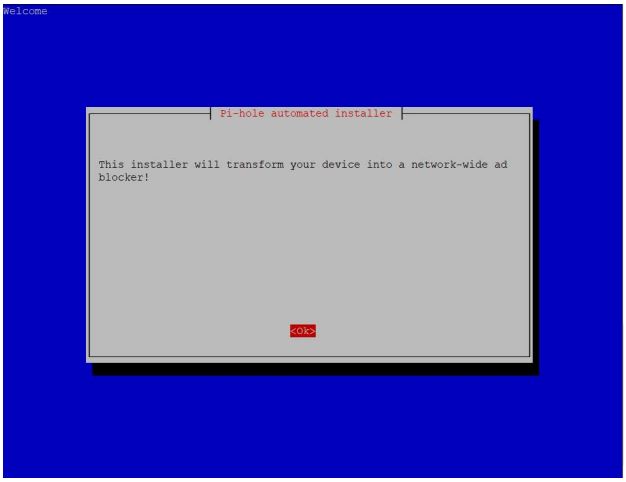
Notes: PI-HOLE stops computers from accessing certain websites, kills unwanted traffic, adverts, bad websites and makes your internet faster.
In some cases your internet router or ISP may not support IPv6
If you have only a IPv4 Router select only IPv4 (Most Compatible)
If you have errors restart the install and def change to IPv4 or change DNS Servers Options
If you Continue to have error run update and upgrade and restart the install

- pi-hole uninstall
- pi-hole restartdns
- pi-hole -r (Re-Configure)
- pi-hole status
- pihole -l off
- pihole disable 10m (minutes) or pihole disable
- cat pihole.log

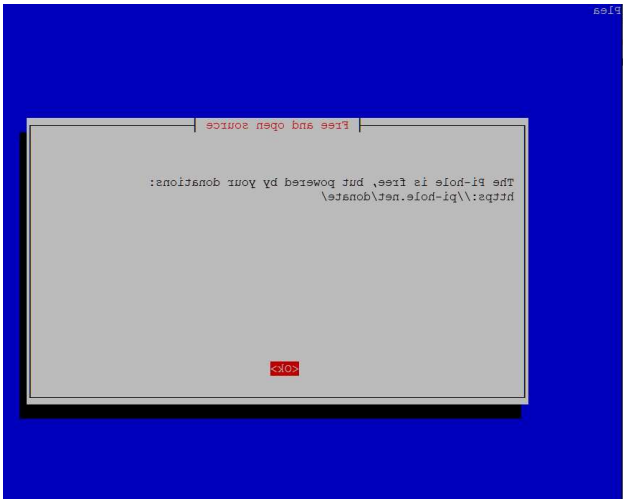

pi@RaspAP: ~
This is a security risk - please login as the 'pi' user and type 'passwd' to set
a new password.
pi@RaspAP:~ $ sudo curl -sSL https://install.pi-hole.net | bash
[i] Root user check
[i] Script called with non-root privileges
The Pi-hole requires elevated privileges to install and run
Please check the installer for any concerns regarding this requirement
Make sure to download this script from a trusted source
[✓] Sudo utility check
[✓] Root user check
[i] Update local cache of available packages...

1. **Start** the Pi-Hole **Installation** (When prompted say y for yes for all defaults)
sudo curl -sSL https://install.pi-hole.net | bash

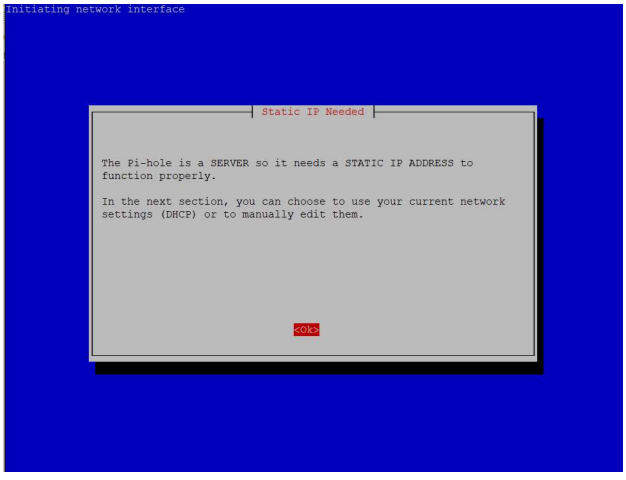
2.Click **OK**



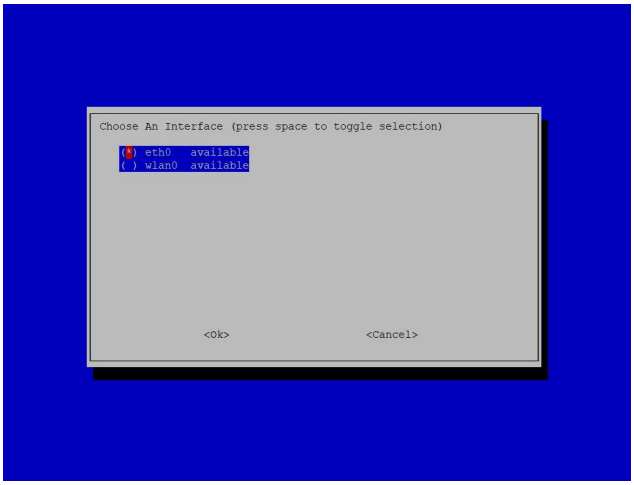
3.Click **OK**



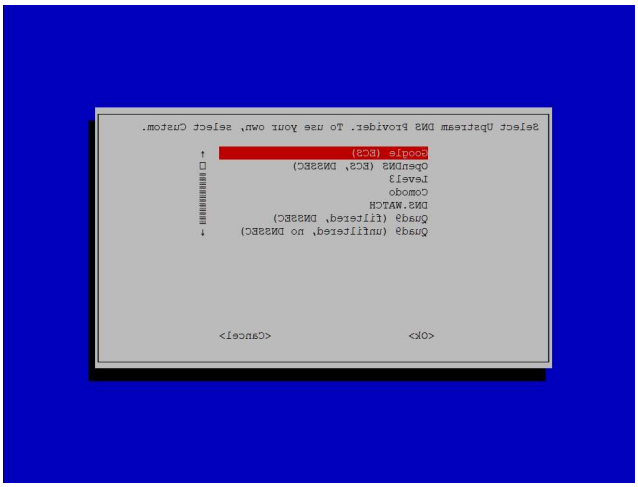
4.Click **OK**


Initiating network interface
Static IP Needed
The Pi-hole is a SERVER so it needs a STATIC IP ADDRESS to function properly.
In the next section, you can choose to use your current network settings (DHCP) or to manually edit them.
<Ok>

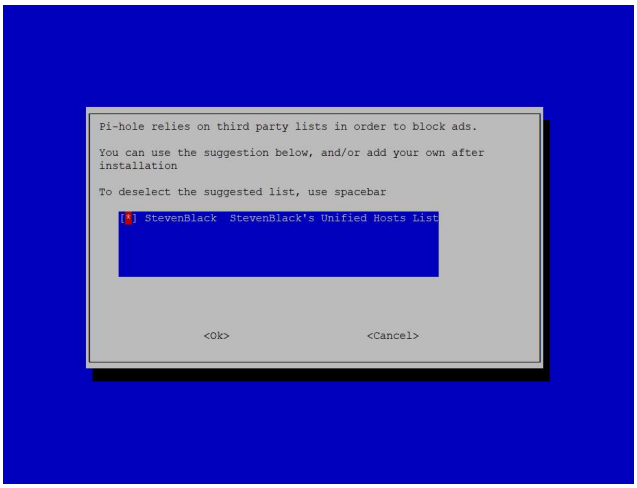
5.Select **ETH0** for wired network Card and Click **OK (If you have WIFI select the other)**



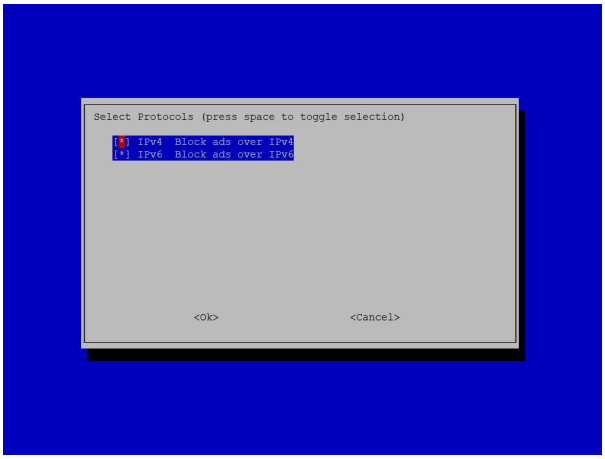
6.Leave **GOOGLE** as default DNS and click **OK**



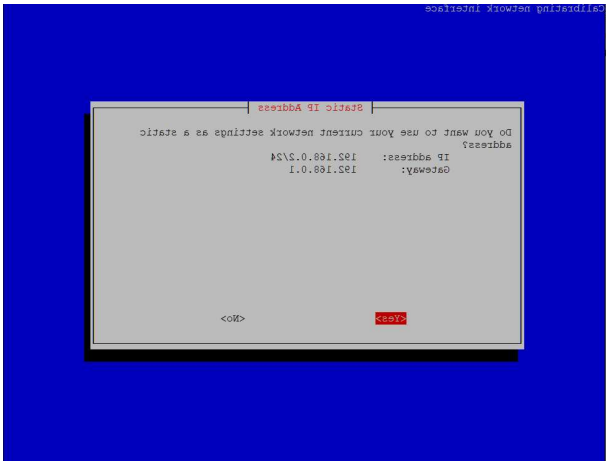
7.Leave the **LISTS** settings as default and click **OK**


Pi-hole relies on third party lists in order to block ads.
You can use the suggestion below, and/or add your own after installation
To deselect the suggested list, use spacebar
[*] StevenBlack StevenBlack's Unified Hosts List
<Ok>
<Cancel>

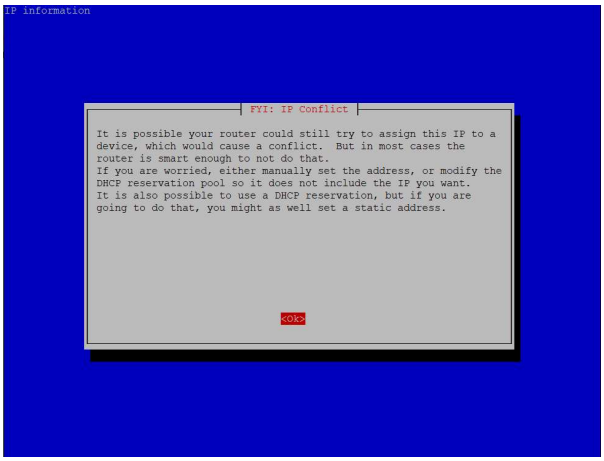
8.Right so this is where it gets tricky, if your **router and ISP support IPV6** then select both options else only select **IPV4** only. You can try both and if you get errors start the install again. Click **OK**



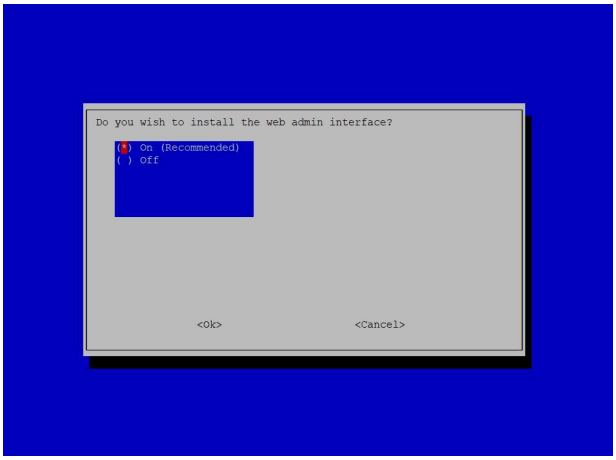
9.Leave as default and click **OK**



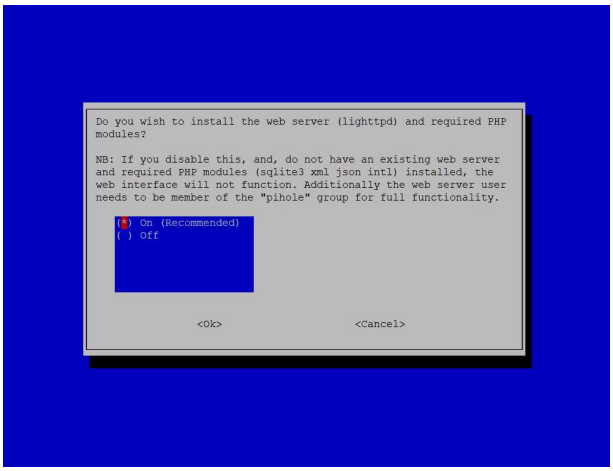
10.Click **OK**


IP information
FYI: IP Conflict
It is possible your router could still try to assign this IP to a
device, which would cause a conflict. But in most cases the
router is smart enough to not do that.
If you are worried, either manually set the address, or modify the
DHCP reservation pool so it does not include the IP you want.
It is also possible to use a DHCP reservation, but if you are
going to do that, you might as well set a static address.
<Ok>

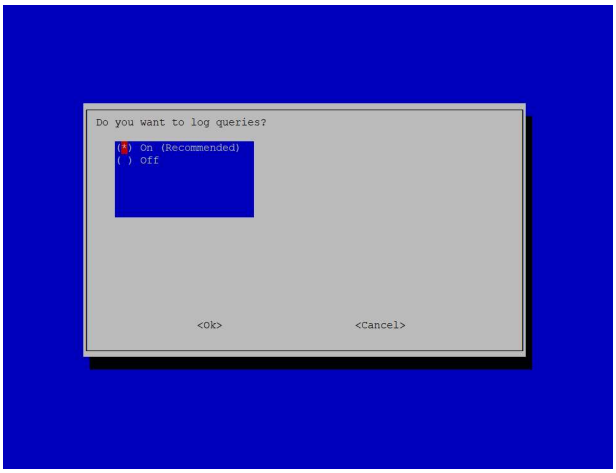
11.Click **OK**



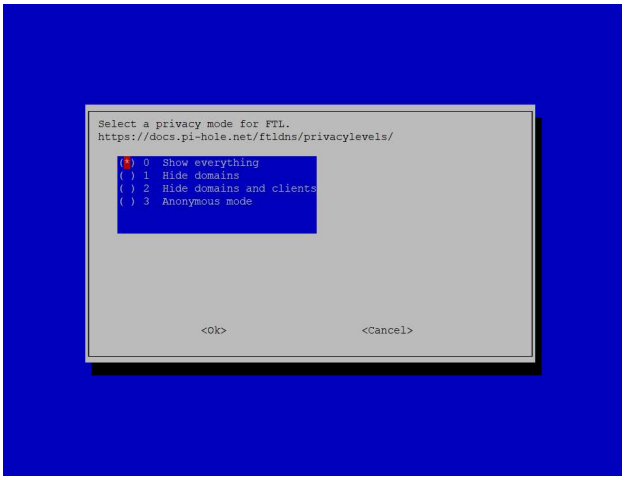
12. Click **OK**


Do you wish to install the web server (lighttpd) and required PHP modules?
NB: If you disable this, and, do not have an existing web server and required PHP modules (sqlite3 xml json intl) installed, the web interface will not function. Additionally the web server user needs to be member of the "pihole" group for full functionality.
(*) On (Recommended)
( ) Off
<Ok>
<Cancel>

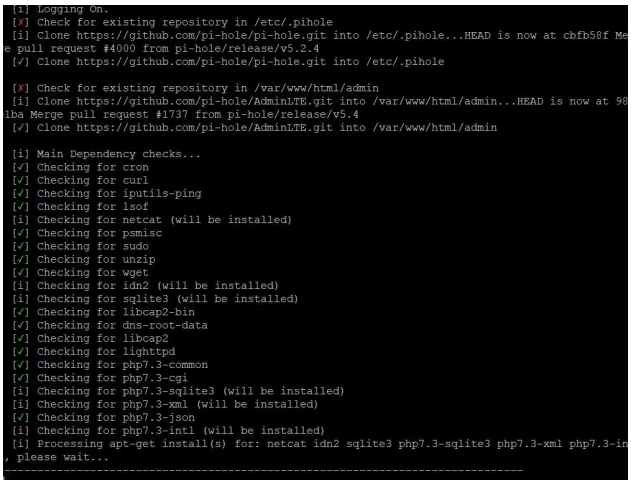
13.Click **OK**



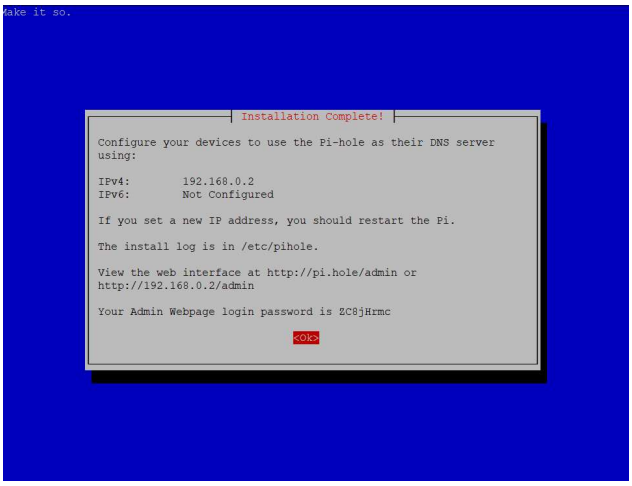
14.Click **OK**


Select a privacy mode for FTL.
https://docs.pi-hole.net/ftldns/privacylevels/
(*) 0 Show everything
( ) 1 Hide domains
( ) 2 Hide domains and clients
( ) 3 Anonymous mode
<Ok>
<Cancel>

15.The System will now **install**


[i] Logging On.
[X] Check for existing repository in /etc/.pihole
[i] Clone https://github.com/pi-hole/pi-hole.git into /etc/.pihole...HEAD is now at cbfb58f Me
e pull request #4000 from pi-hole/release/v5.2.4
[✓] Clone https://github.com/pi-hole/pi-hole.git into /etc/.pihole
[X] Check for existing repository in /var/www/html/admin
[i] Clone https://github.com/pi-hole/AdminLTE.git into /var/www/html/admin...HEAD is now at 98
iba Merge pull request #1737 from pi-hole/release/v5.4
[✓] Clone https://github.com/pi-hole/AdminLTE.git into /var/www/html/admin
[i] Main Dependency checks...
[✓] Checking for cron
[✓] Checking for curl
[✓] Checking for iputils-ping
[✓] Checking for lsof
[i] Checking for netcat (will be installed)
[✓] Checking for psmisc
[✓] Checking for sudo
[✓] Checking for unzip
[✓] Checking for wget
[i] Checking for idn2 (will be installed)
[i] Checking for sqlite3 (will be installed)
[✓] Checking for libcap2-bin
[✓] Checking for dns-root-data
[✓] Checking for libcap2
[✓] Checking for lighttpd
[✓] Checking for php7.3-common
[✓] Checking for php7.3-cgi
[i] Checking for php7.3-sqlite3 (will be installed)
[i] Checking for php7.3-xml (will be installed)
[✓] Checking for php7.3-json
[i] Checking for php7.3-intl (will be installed)
[i] Processing apt-get install(s) for: netcat idn2 sqlite3 php7.3-sqlite3 php7.3-xml php7.3-in
, please wait...

16.When completed write down the **PASSWORD** and **WEB ADMIN URL** and the click **OK**


Make it so.
Installation Complete!
Configure your devices to use the Pi-hole as their DNS server
using:
IPv4: 192.168.0.2
IPv6: Not Configured
If you set a new IP address, you should restart the Pi.
The install log is in /etc/pihole.
View the web interface at http://pi.hole/admin or
http://192.168.0.2/admin
Your Admin Webpage login password is ZC8jHrmc
<Ok>

Example:
PASSWORD = ZC8jHrmc
URL = http://192.168.0.2/admin

5. Change the **password** to nothing (Just enter with blank)
pihole -a -p

6. Change **Long Term DATA** Storage to 1 day kept. (Add the following line to the end of the file)
sudo nano /etc/pihole/pihole-FTL.conf

##
MAXDBDAYS = 1
##

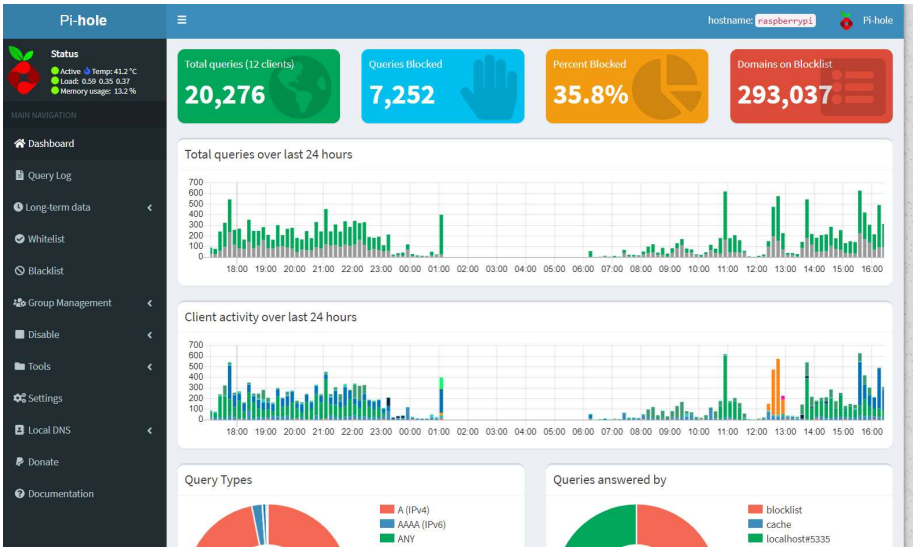
7. **Reboot** the system
sudo reboot

8. RUN THE RECOMENDED **UPDATE AGAIN**
sudo apt-get update

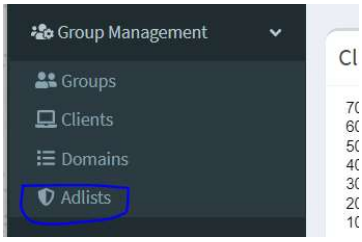
9. **Reboot** the system
sudo reboot

10.To Access the Pi-Hole **Open your Internet Browser** and open one of the below.

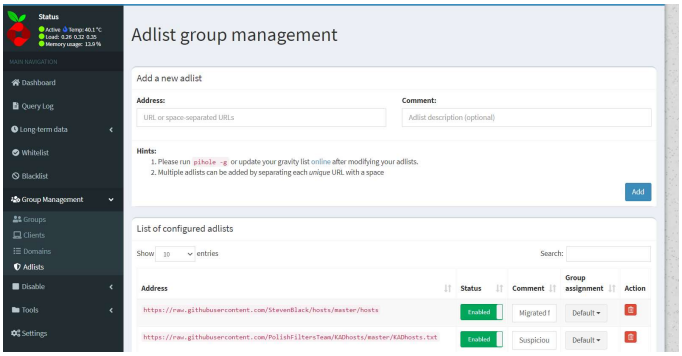
http://pi.hole/admin
http://192.168.0.2/admin
http://raspap/



11. Click on **GROUP MANAGEMENT** and **CLICK ON ADLIST**



12. **Add you lists** and when done remember to update



13.Below is a list of websites where most people get their **adlists**, these lists vary from adverts, telemetry and bad sites for blocking. (No warranty given, use at own risk)

https://firebog.net/ (Select the green ones)
https://github.com/thomasbnt/raspihostblock
https://github.com/LunarWatcher/Pihole-blocklists/raw/master/desktop-blocklist.txt
https://oisd.nl/ (I use this one)
https://ftpihole.com/lists/

14. **Update the Adlists** when finished loading lists *(This makes the lists work)*
pihole -g
or
http://192.168.0.6/admin/gravity.php

14. **Create a CRONTAB** to update the Adlist once a week and Reboot once a week
sudo crontab -u pi -e

##################################
15 0 * * 1 /usr/local/bin/pihole -g
##################################

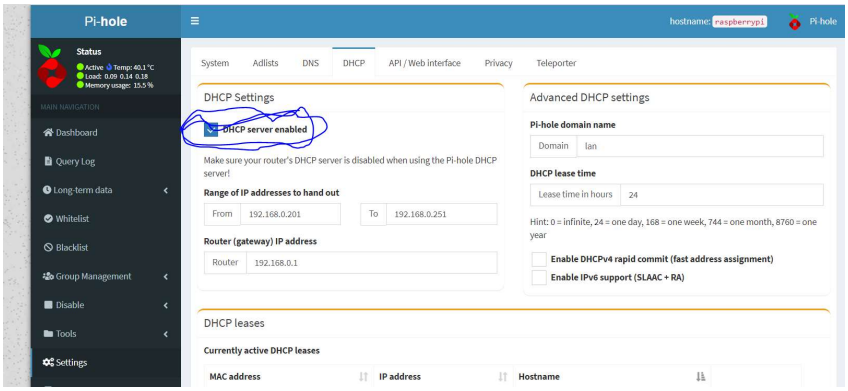
15. **Restart** the **CronTab** service
sudo service cron restart

SETTING DHCP AND DNS TO USE PI-HOLE

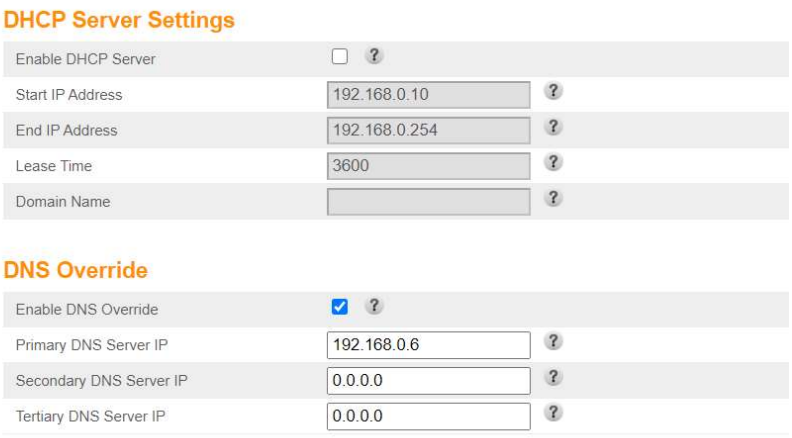
Resources Guides:

Notes: Once you setup PI-HOLE you may want to opt to use PI-HOLE DHCP or JUST DNS

1.To **enable DHCP** on **PI-Hole** click on settings and DHCP and enable it
WARNING: Only one DHCP can be running on your network. The reason most people use Pi-Hole DHCP is to have more control on their network and to see all the connections on it. If you are running RaspAP on another server the connection will only see one network.

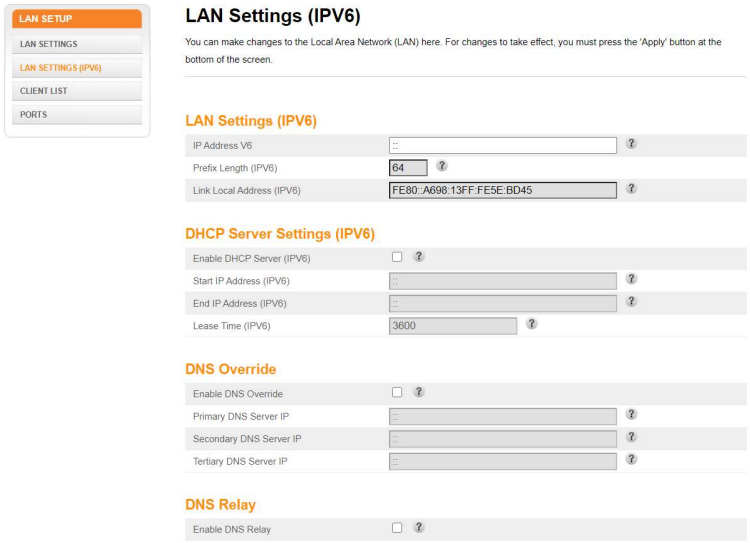


2.To **disable DHCP on your router,** login and find the setting to disable the DHCP. If possible also **point the DNS** to your **PI-HOLE** as you see below.



WARNING: YOU CAN ONLY HAVE 1 (ONE) DHCP SERVER ON YOUR NETWORK AT ANY TIME

3.In some cases some people **disable IPV6 on their router**, but only if they have issues or want to force al users on IPV4.



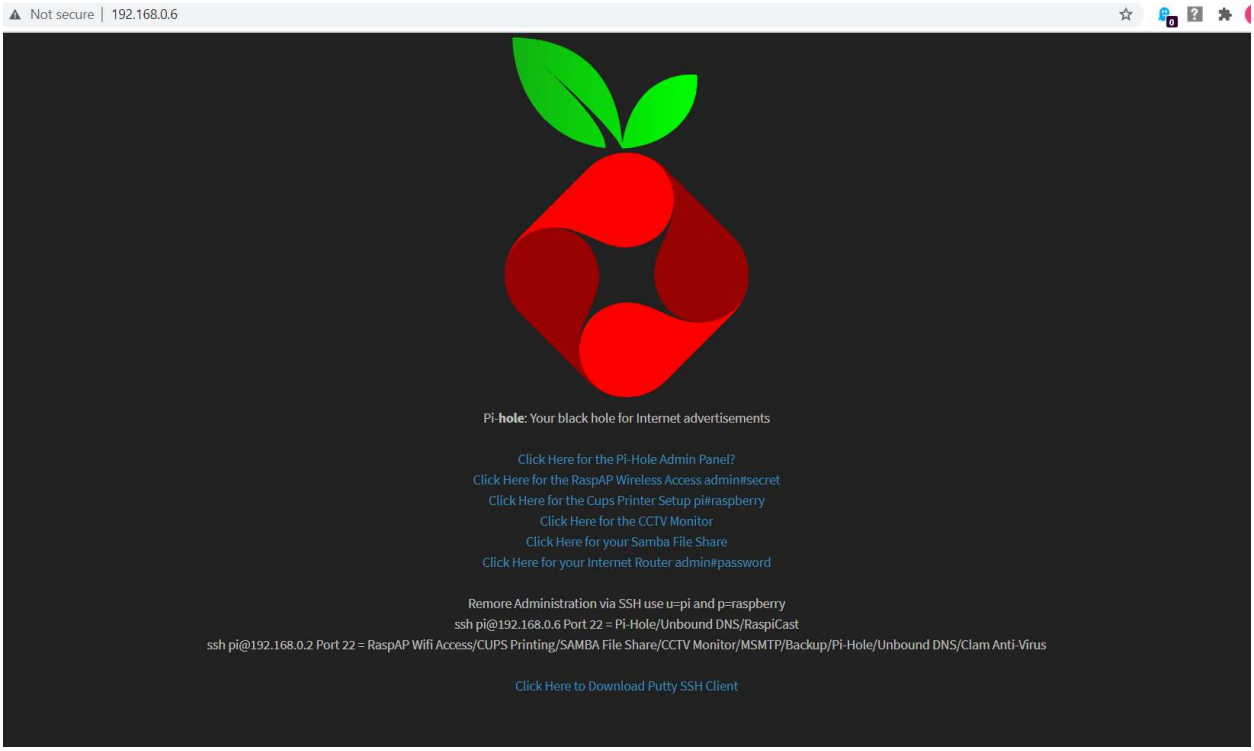
Finished

SETUP PI WEBSERVER FOR EASY ACCESS

Resources Guides:

Notes: We setup the pi server webs page to reflect all our changes for ease of use

---


Not secure | 192.168.0.6
Pi-hole: Your black hole for Internet advertisements
Click Here for the Pi-Hole Admin Panel?
Click Here for the RaspAP Wireless Access admin#secret
Click Here for the Cups Printer Setup pi#raspberry
Click Here for the CCTV Monitor
Click Here for your Samba File Share
Click Here for your Internet Router admin#password
Remore Administration via SSH use u=pi and p=raspberry
ssh pi@192.168.0.6 Port 22 = Pi-Hole/Unbound DNS/RaspiCast
ssh pi@192.168.0.2 Port 22 = RaspAP Wifi Access/CUPS Printing/SAMBA File Share/CCTV Monitor/MSMTP/Backup/Pi-Hole/Unbound DNS/Clam Anti-Virus
Click Here to Download Putty SSH Client

1. **Edit the website index** file
sudo nano /var/www/html/pihole/index.php

2. Find and **change the following** section to include the following

```
#####################################################

        <p>Pi-<strong>hole</strong>: Your black hole for Internet advertisements</p>
<br>
<a href='http://192.168.0.2/admin' target='_blank'>Click Here for the Pi-Hole Admin Panel?</a>
<br>
<a href='http://192.168.0.6/admin' target='_blank'>Click Here for the Secondary Pi-Hole Admin Panel?
</a>
```

```
<br><a href='http://192.168.0.2:8082' target='_blank'>Click Here for the RaspAP Wireless Access admin#secret</a>
<br><a href='http://192.168.0.2:631/' target='_blank'>Click Here for the Cups Printer Setup pi#raspberry</a>
<br><a href='http://192.168.0.2:8081/' target='_blank'>Click Here for the CCTV Monitor pi#raspberry</a>
<br><a href='file://192.168.0.2/share/' target='_blank'>Click Here for your Samba File Share</a>
<br><a href='http://192.168.0.1' target='_blank'>Click Here for your Internet Router admin#password</a>
<br><br>
<p>To connect to Servers to admin via SSH use u=pi and p=raspberry
<br>
192.168.0.2:22 = RaspAP Wifi AP or PiHole Unbound DNS and CUPS Printing and SAMBA File Share and CCTV Monitor
<br>
192.168.0.6:22 = Secondary Pi-Hole and Unbound DNS and RaspiCast
<br>
</p>
<br><a href='https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html' target='_blank'>Click Here to Download Putty SSH Client</a>

    </body>
  </html>
```

```
#####################################################
```

3.**Save** you settings

4.Now visit your **start webpage**
http://192.168.0.2

Finished

UNBOUND DNS SERVER

Resources Guides:
https://docs.pi-hole.net/guides/dns/unbound/
https://awesomeopensource.com/project/anudeepND/pihole-unbound
https://docs.pi-hole.net/ftldns/dns-cache/
https://www.smarthomebeginner.com/pi-hole-setup-guide/

Notes: sudo apt remove unbound
---

1. Run the **Installer and reboot when done**
sudo apt install unbound
sudo reboot

2. Get the **Root Hints**
wget https://www.internic.net/domain/named.root -qO- | sudo tee /var/lib/unbound/root.hints

3. **Edit the config** file and modify it with the below settings
sudo nano /etc/unbound/unbound.conf.d/pi-hole.conf

```
##############################################################
server:
    # If no logfile is specified, syslog is used
    # logfile: "/var/log/unbound/unbound.log"
    verbosity: 0

    interface: 127.0.0.1
    port: 5335
    do-ip4: yes
    do-udp: yes
    do-tcp: yes

    # May be set to yes if you have IPv6 connectivity??????????????????????????????????
    do-ip6: no

    # You want to leave this to no unless you have *native* IPv6. With 6to4 and??????????
    # Terredo tunnels your web browser should favor IPv4 for the same reasons
    prefer-ip6: no

    # Use this only when you downloaded the list of primary root servers!
    # If you use the default dns-root-data package, unbound will find it automatically
    #root-hints: "/var/lib/unbound/root.hints"
```

```
    # Trust glue only if it is within the server's authority
    harden-glue: yes

    # Require DNSSEC data for trust-anchored zones, if such data is absent, the zone becomes BOGUS
    harden-dnssec-stripped: yes

    # Don't use Capitalization randomization as it known to cause DNSSEC issues sometimes
    # see https://discourse.pi-hole.net/t/unbound-stubby-or-dnscrypt-proxy/9378 for further details
    use-caps-for-id: no

    # Reduce EDNS reassembly buffer size.
    # Suggested by the unbound man page to reduce fragmentation reassembly problems
    edns-buffer-size: 1472

    # Perform prefetching of close to expired message cache entries
    # This only applies to domains that have been frequently queried
    prefetch: yes

    # One thread should be sufficient, can be increased on beefy machines. In reality for most users running on small networks or on a single machine, it should be unnecessary to seek performance enhancement by increasing num-threads above 1.
    num-threads: 1

    # Ensure kernel buffer is large enough to not lose messages in traffic spikes
    so-rcvbuf: 1m

    # Ensure privacy of local IP ranges
    private-address: 192.168.0.0/16
    private-address: 169.254.0.0/16
    private-address: 172.16.0.0/12
    private-address: 10.0.0.0/8
    private-address: fd00::/8
    private-address: fe80::/10
###########################################################################
```

Save your settings

4. **Restart Unbound service**

```
sudo service unbound restart
```

5. **CHECK AND TEST** SHOULD SHOW = NOERROR

```
dig pi-hole.net @127.0.0.1 -p 5335
```

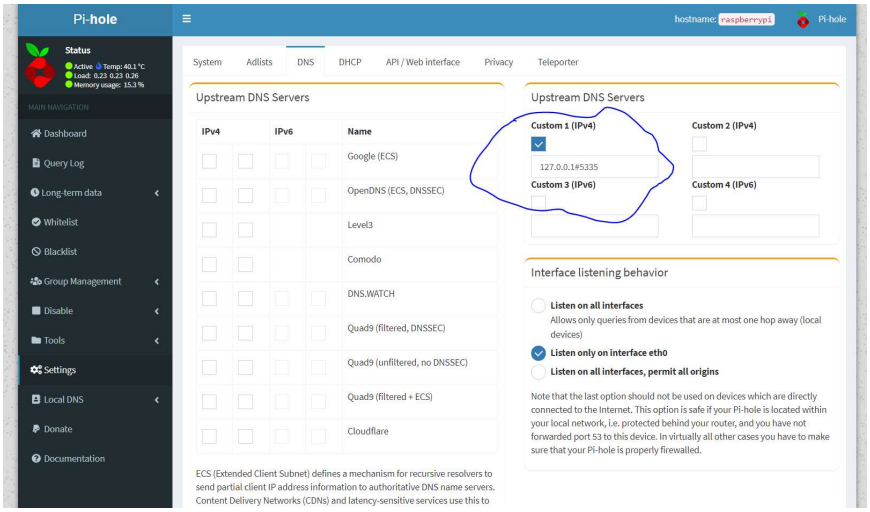
6.**CHECK AND TEST** SHOULD SHOW = SERVFAIL

```
dig sigfail.verteiltesysteme.net @127.0.0.1 -p 5335
```

7. **CHECK AND TEST** SHOULD SHOW = NOERROR

```
dig sigok.verteiltesysteme.net @127.0.0.1 -p 5335
```

8. In **http://PI-HOLE/Admin** go to **Settings** and set custom **DNS** to
127.0.0.1#5335


Pi-hole
hostname: raspberrypi
Status
Active Temp: 40.1 °C
Load: 0.23 0.23 0.26
Memory usage: 15.3 %
MAIN NAVIGATION
Dashboard
Query Log
Long-term data
Whitelist
Blacklist
Group Management
Disable
Tools
Settings
Local DNS
Donate
Documentation
System
Adlists
DNS
DHCP
API / Web interface
Privacy
Teleporter
Upstream DNS Servers
IPv4
IPv6
Name
Google (ECS)
OpenDNS (ECS, DNSSEC)
Level3
Comodo
DNS.WATCH
Quad9 (filtered, DNSSEC)
Quad9 (unfiltered, no DNSSEC)
Quad9 (filtered + ECS)
Cloudflare
ECS (Extended Client Subnet) defines a mechanism for recursive resolvers to send partial client IP address information to authoritative DNS name servers. Content Delivery Networks (CDNs) and latency-sensitive services use this to
Upstream DNS Servers
Custom 1 (IPv4)
127.0.0.1#5335
Custom 2 (IPv4)
Custom 3 (IPv6)
Custom 4 (IPv6)
Interface listening behavior
Listen on all interfaces
Allows only queries from devices that are at most one hop away (local devices)
Listen only on interface eth0
Listen on all interfaces, permit all origins
Note that the last option should not be used on devices which are directly connected to the Internet. This option is safe if your Pi-hole is located within your local network, i.e. protected behind your router, and you have not forwarded port 53 to this device. In virtually all other cases you have to make sure that your Pi-hole is properly firewalled.

9. Run the next to **Fix the DNS** and Resolve
sudo systemctl status unbound-resolvconf.service (press q to exit)
sudo systemctl disable unbound-resolvconf.service
sudo systemctl stop unbound-resolvconf.service
sudo systemctl restart dhcpcd

9. **Check** if the local system uses correct **DNS**
cat /etc/resolv.conf

10. **Disabling Pi Hole caching** requires setting the cache size to 0 in (was 10000)
sudo nano /etc/dnsmasq.d/01-pihole.conf

```
##########################################################
cache-size=0
##########################################################
```

11. **Restart** the UNBOUND **Service**
sudo service unbound restart

12. **Create a Script** to update all the PI-HOLE lists every week for changes and DNS root hints.
sudo nano /usr/local/sbin/update-all-list.sh

```
##########################################################
#!/bin/sh
# Remove the hash if you are downloading the root hints else its automatic
# wget https://www.internic.net/domain/named.root -qO- | sudo tee /var/lib/unbound/root.hints
/opt/whitelist/scripts/whitelist.sh >/dev/null
```

/opt/whitelist/scripts/referral.sh >/dev/null
###

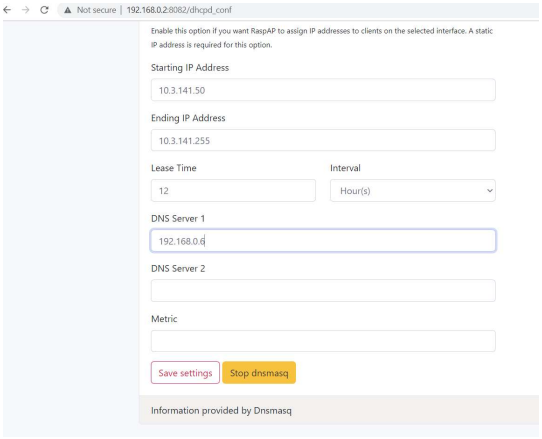
13.**Make** the file **executable**
sudo chmod +x /usr/local/sbin/update-all-list.sh

14. Create a **CRONTAB** to run the Script
sudo crontab -u pi -e

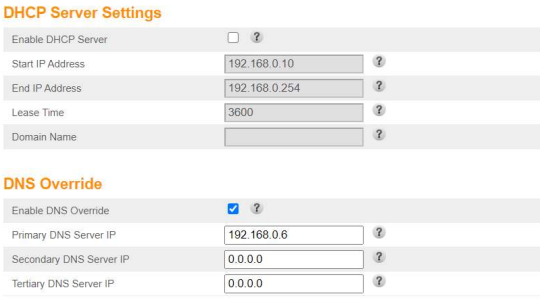
#################################
0 0 * * 1 /usr/local/sbin/update-all-list.sh
#################################

15. **Restart** the **CronTab** service
sudo service cron restart

16. OPTIONAL: Open RaspAP if you installed it and check the **DHCP DNS** is set to 192.168.0.2



17. OPTIONAL: Change your **router DHCP** to use the local DNS server



Finished

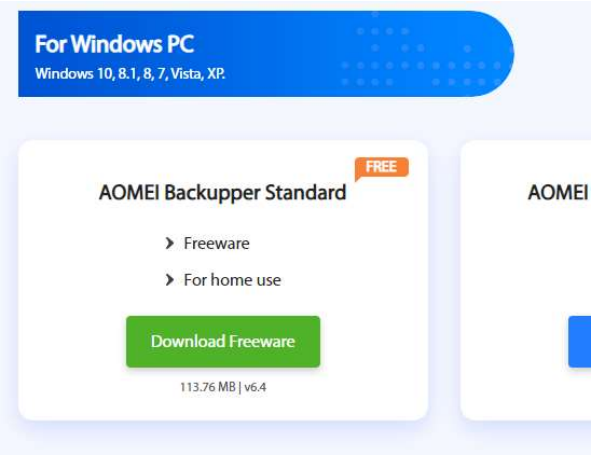
DISASTER RECOVER (WHEN YOUR USB DIES)

Resources Guides:
https://www.aomeitech.com/aomei-backupper.html

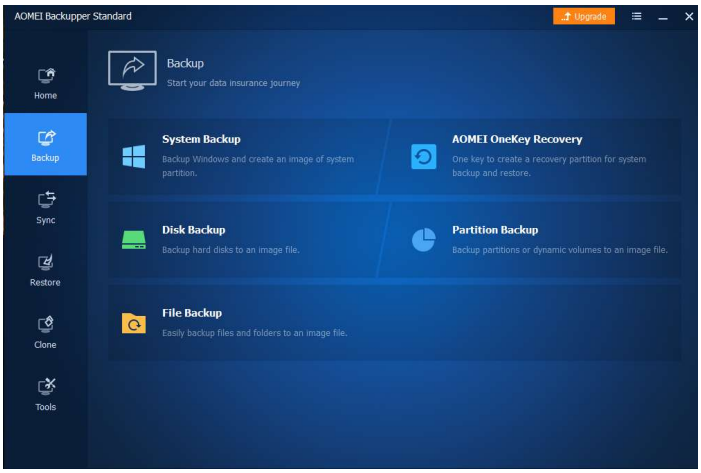
Notes: You should have a spare USB on standby or at very least backed up your installation USB, this will allow you to restore to another USB.

WARNING: BEFORE RESTORING YOUR USB DRIVE, MAKE SURE YOU HAVE DOWNLOADED ALL THE FILES FROM YOUR GOOGLE BACKUP GDRIVE AND PUT IN A SAFE LOCATION TO RESTORE LATER. IF YOU SYNC An EMPTY BACKUP, YOU WILL LOOSE ALL YOUR GDRIVE DATA!

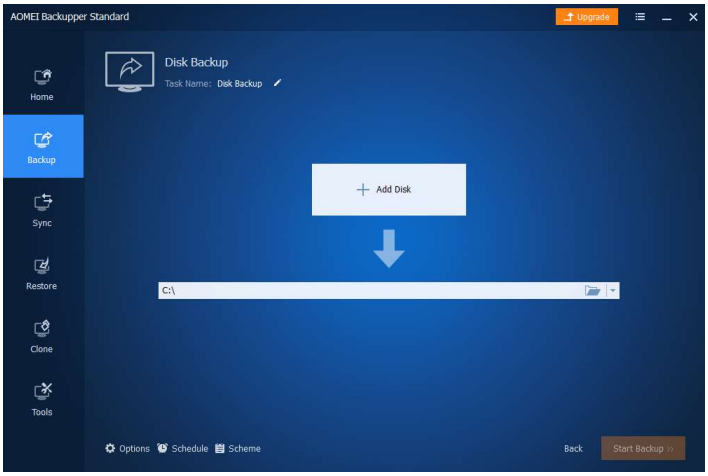
1.Get Free **AOMEI Backupper Software**
https://www.aomeitech.com/aomei-backupper.html



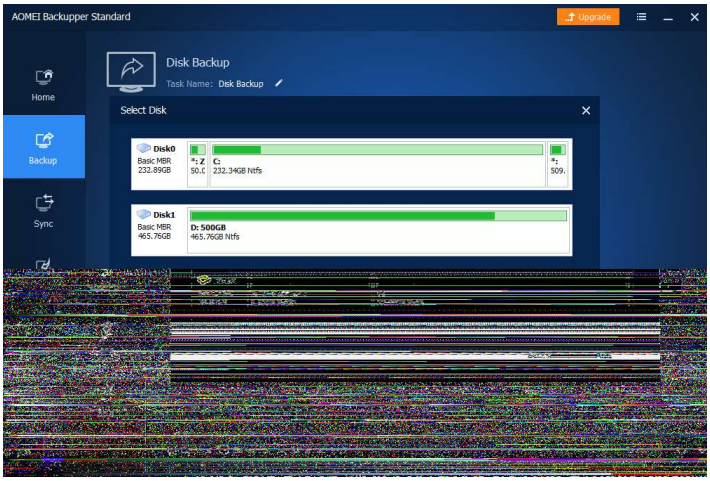
2.After you have installed run the program and click on **BACKUP** and select **DISK BACKUP**



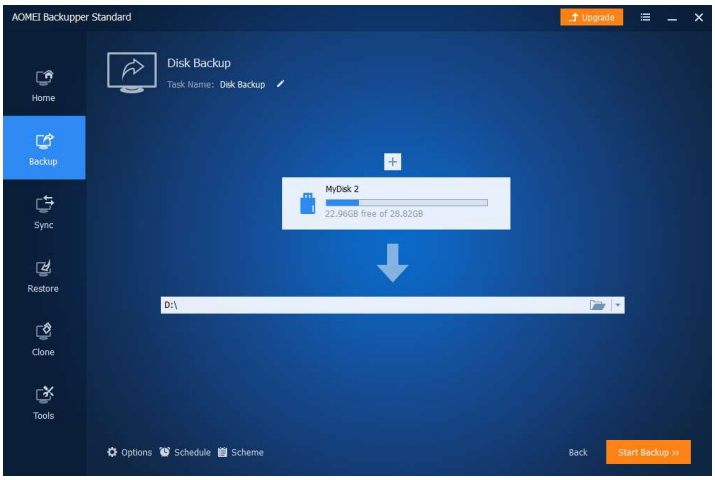
3.Click **ADD DISK**



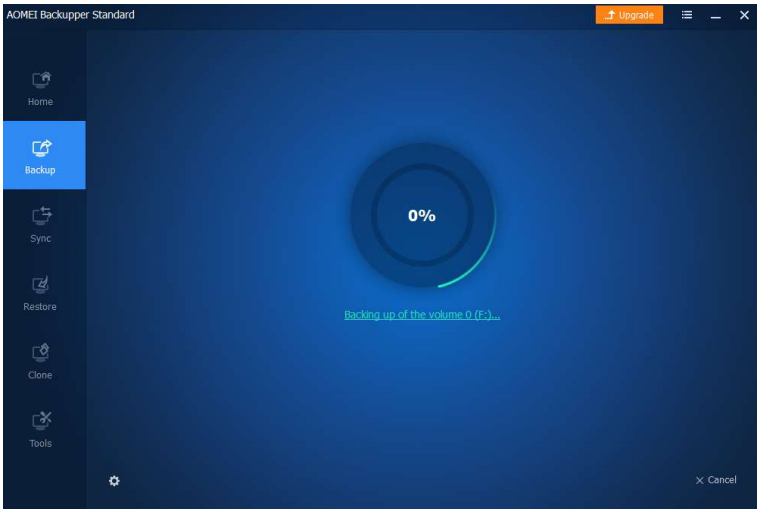
4.Select the **USB DRIVE** and **CLICK ADD**



5.Select where you wish to **SAVE THE DATA** and click **START BACKUP**



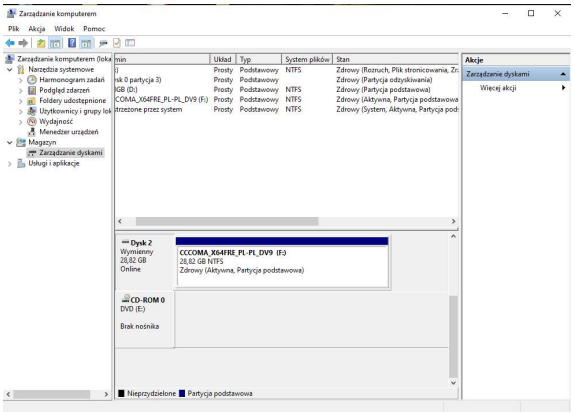
6.The USB will now be backed up and you can **restore** another USB for **Disaster Recovery**



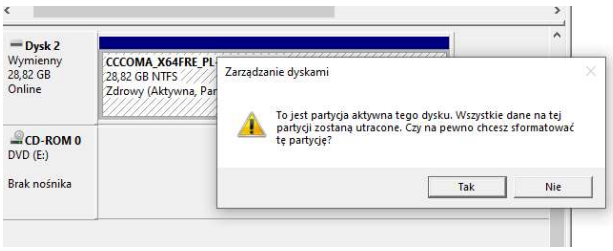
NOTE YOU SHOULD ALSO CLONE YOUR FINISHED PI DISK TO ANOTHER USB

In order for us not to get mixed up with the USB drives I will format and relabel the USB(OPTIONAL)

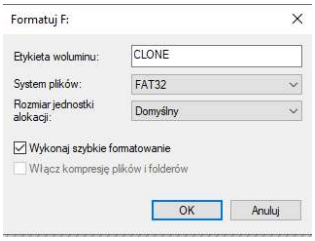
1.Open **Computer Manager** and then click on **DISK MANAGEMENT** (or type this in the win search bar)



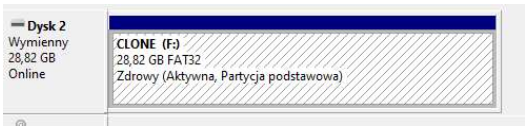
2.**Right Click** on the **USB Drive** you wish to **format** and click format
You will get a message that all the data will be destroyed. Make sure this is the correct USB or drive before you click **YES**



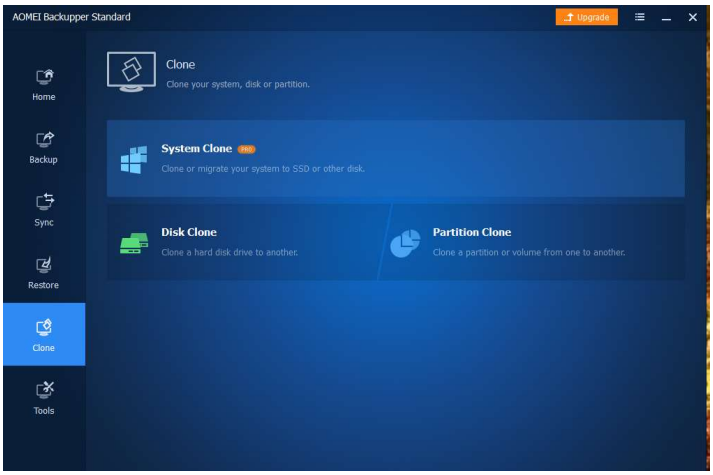
3.**Change** the **Label** to **CLONE** and select **FAT32** and click OK and again OK



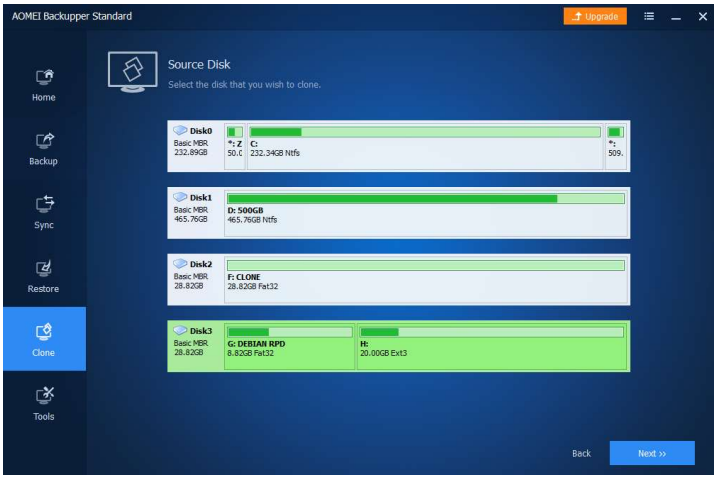
4.When done you should now have a **USB** called **CLONE**



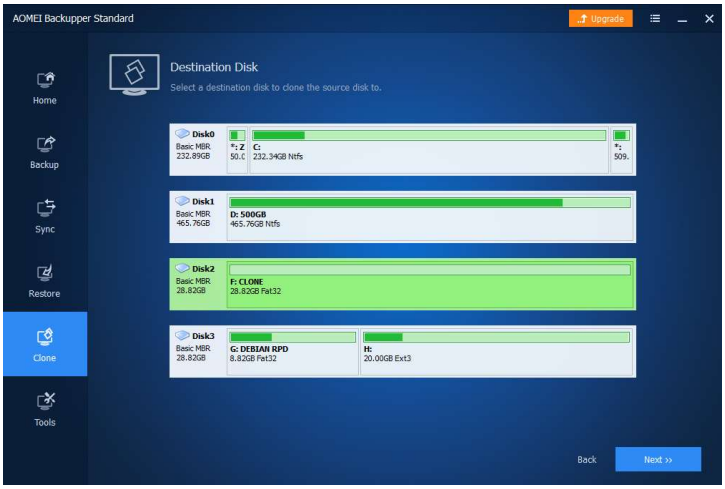
5.**Plug in** your Raspberry Pi **USB** and start **AOMEI Backupper**, then click on **CLONE** and **DISK CLONE**



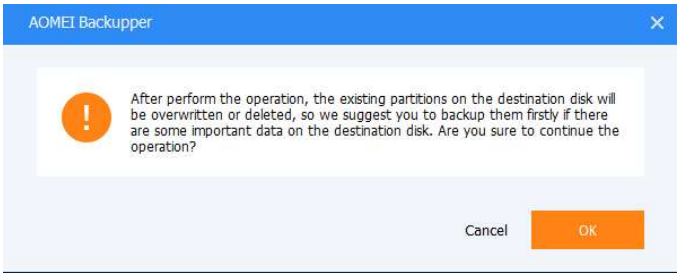
6.Select the **SOURCE** disk **DEBIAN RPD** and click **NEXT**



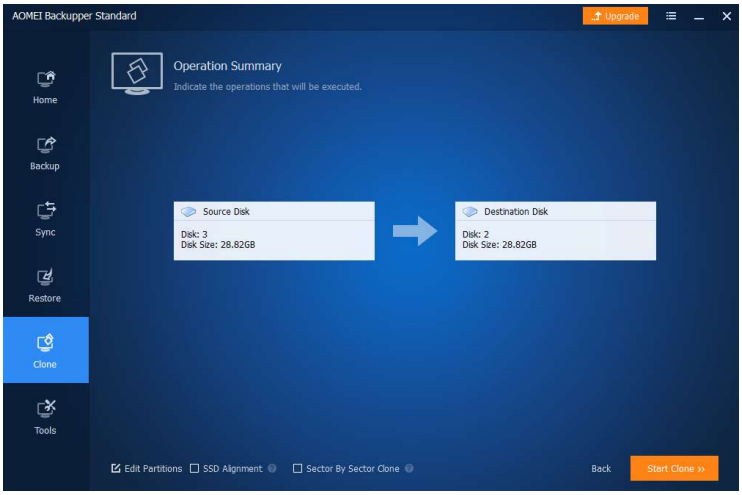
7.Select the **DESTINATION DISK** we named **CLONE**



8.Click on **OK** if you *selected the correct disks or you will lose data*


AOMEI Backupper
After perform the operation, the existing partitions on the destination disk will be overwritten or deleted, so we suggest you to backup them firstly if there are some important data on the destination disk. Are you sure to continue the operation?
Cancel
OK

9.Click on **START CLONE**



10.The CLONE process will now start and when **finished** you will have a CLONED DISASTER RECOVERY USB spare for when things go wrong.

SETTING UP RASPBERRY PI ON A SSD CARD

Resources Guides:

Notes:

---

1. **Download** the Raspberry Pi Imager
https://www.raspberrypi.org/%20downloads/

2. Click **Choose OS**
Select Raspberry Pi OS (Other)
Select Raspberry Pi OS Lite (32Bit)

3. Click CHOOSE **SD CARD**
Select your SD card (This will destroy all data on it so select correct)

4. Click **WRITE**
You will be prompted all data will be destroyed

5. Click **YES**
(Wait until completed 100%)
When done insert you SD card into your Pi

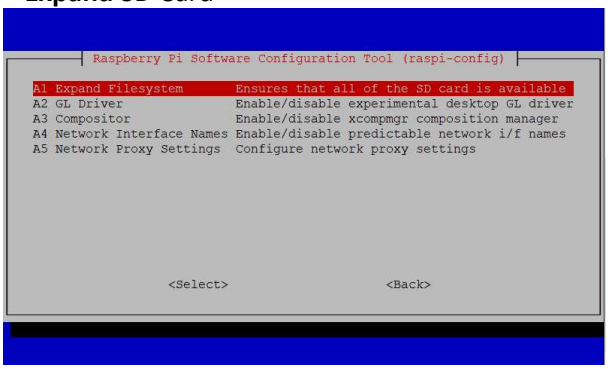
6. Connect you Pi Zero with **keyboard and Monitor** , Power On and login
Username **pi** and password **raspberry**

7. **Edit** the dhcpca.conf file and enter a static IP for your network
sudo vi etc/dhcpcd.conf

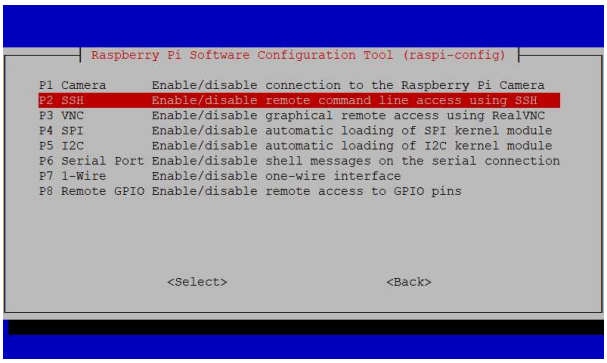
```
#######################################################################
# Example static IP configuration:
interface eth0
static ip_address=192.168.0.2/24
static ip6_address=fd51:42f8:caae:d92e::ff/64
static routers=192.168.0.1
static domain_name_servers=192.168.0.1 8.8.8.8 fd51:42f8:caae:d92e::1
#######################################################################
```

8. Run the following command to configure you Pi
sudo raspi-config

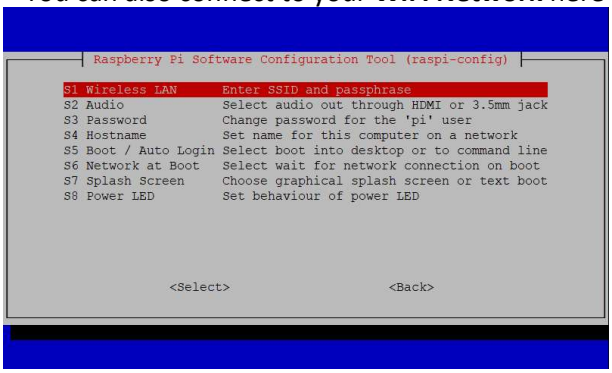
* **Expand** SD Card


Raspberry Pi Software Configuration Tool (raspi-config)
A1 Expand Filesystem Ensures that all of the SD card is available
A2 GL Driver Enable/disable experimental desktop GL driver
A3 Compositor Enable/disable xcompmgr composition manager
A4 Network Interface Names Enable/disable predictable network i/f names
A5 Network Proxy Settings Configure network proxy settings
<Select>
<Back>

* Enable **SSH**


Raspberry Pi Software Configuration Tool (raspi-config)
P1 Camera Enable/disable connection to the Raspberry Pi Camera
P2 SSH Enable/disable remote command line access using SSH
P3 VNC Enable/disable graphical remote access using RealVNC
P4 SPI Enable/disable automatic loading of SPI kernel module
P5 I2C Enable/disable automatic loading of I2C kernel module
P6 Serial Port Enable/disable shell messages on the serial connection
P7 1-Wire Enable/disable one-wire interface
P8 Remote GPIO Enable/disable remote access to GPIO pins
<Select>
<Back>

* You can also connect to your **WIFI Network** here if you are not using eth0


Raspberry Pi Software Configuration Tool (raspi-config)
S1 Wireless LAN Enter SSID and passphrase
S2 Audio Select audio out through HDMI or 3.5mm jack
S3 Password Change password for the 'pi' user
S4 Hostname Set name for this computer on a network
S5 Boot / Auto Login Select boot into desktop or to command line
S6 Network at Boot Select wait for network connection on boot
S7 Splash Screen Choose graphical splash screen or text boot
S8 Power LED Set behaviour of power LED
<Select>
<Back>

9. **Reboot** the system

```
sudo reboot
```

10.Dont forget to **make a backup** of your SD card when done
AOMEI Backupper Software

11.**Download and install Putty** on your workstation and connect to your system **<ipaddress>:22**
https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

Finished

OTHER TOPICS NOT COVERED IN THIS BOOK

KODI
https://kodi.wiki/view/HOW-TO:Install_Kodi_on_Raspberry_Pi

OSMC
https://www.maketecheasier.com/install-osmc-on-raspberry-pi/

MAILSERVER POSTFIX
https://raspberrytips.com/mail-server-raspberry-pi/

KALI LINUX PI
https://pimylifeup.com/raspberry-pi-kali-linux/

RASPBERRY PI LTE INTERNET MODEM
https://www.raspberrypi.org/forums/viewtopic.php?t=210724

RASPBERRY PI USB NAS SERVER
https://thepi.io/how-to-use-your-raspberry-pi-as-a-nas-box/

RASPBERRY PI WEBSERVER
https://www.raspberrypi.org/documentation/remote-access/web-server/nginx.md
https://www.howtoforge.com/how-to-install-osclass-with-nginx-on-ubuntu-1804/

INSTALLING SSL CERTIFICATES IN CUPS
https://serverfault.com/questions/883918/https-ssl-not-working-with-cups
https://letsencrypt.org

RASPICAST (THIS WILL ONLY WORK ON A REAL PI DEVICE)
https://www.instructables.com/Raspberry-Pi-As-Chromecast-Alternative-Raspicast/
https://play.google.com/store/apps/details?id=at.huber.raspicast
https://pimylifeup.com/raspberry-pi-chromecast/

RASPBERRY CAST (THIS WILL ONLY WORK ON A REAL PI DEVICE)
https://github.com/vincelwt/RaspberryCast
https://www.circuitstoday.com/raspberry-pi-music-player

SETTING UP WIFI ON A RASPBERRY PI COMMAND LINE
https://www.raspberrypi.org/documentation/configuration/wireless/wireless-cli.md

SETTING UP KODI ON YOUR RASPBERRY PI AND LINUX SYSTEMS
https://www.linuxbabe.com/desktop-linux/install-kodi-debian-8-ubuntu

---

BONUS MATERIAL INSTALLING KODI (TV)

WARNING NOT TESTED – STILL UNDER REVIEW I WOULD RECOMMEND A HDD AND NOT A SD OR USB

Resources Guides:

https://www.linuxbabe.com/desktop-linux/install-kodi-debian-8-ubuntu
http://iwearshorts.com/blog/raspberry-pi-setting-up-your-audio/
https://github.com/iptv-org/iptv
https://discourse.pi-hole.net/t/host-website-alongside-pi-hole-interface/31832

Notes: Building your system as a media center TV
sudo alsamixer
sudo nano /boot/firmware/config.txt
aplay /usr/share/sounds/alsa/Noise.wav
sudo nano /boot/firmware/config.txt
sudo nano /etc/lighttpd/lighttpd.conf
sudo systemctl restart kodi sudo systemctl restart kodi

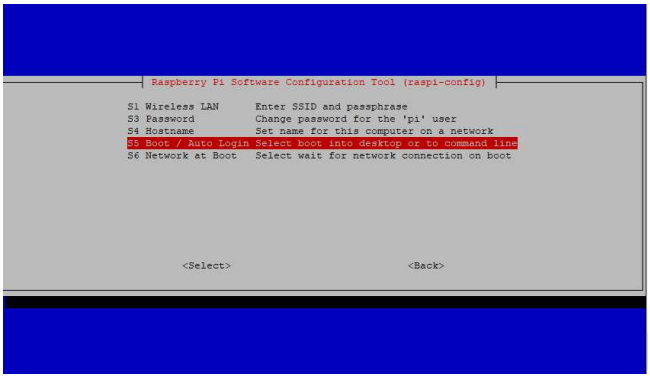
WARNING: IF YOU HAVE CLAM AV SCANNING IT WILL GRIND YOUR SYSTEM TO A HALT WITH USB

---

1. First make sure your sound is working. I found my **sound was muted**. The easy way of checking is to go to your Desktop and clicking on the volume button on the top right.

2.If you selected command line then enable the desktop from **raspi-config** when done disable it again.
sudo raspi-config

Select 1
Select 5


Raspberry Pi Software Configuration Tool (raspi-config)
S1 Wireless LAN Enter SSID and passphrase
S3 Password Change password for the 'pi' user
S4 Hostname Set name for this computer on a network
S5 Boot / Auto Login Select boot into desktop or to command line
S6 Network at Boot Select wait for network connection on boot
<Select>
<Back>

3.Once you have done this and still no sound **install alsa-utils**
sudo apt-get install alsa-utils

4.For my Dell Wyse I needed to enable the **front sound port** as the HDMI is disabled
echo 'pcm.!default front:SB' > ~/.asoundrc

5.Next **edit** the following file and added (You may need to find your driver mine was **snd-hda-intel)**
cat /proc/asound/modules

sudo nano /etc/modprobe.d/alsa-base.conf

##
options **snd-hda-intel** model=generic
##

6.You can **test** the sound with the following to see if its working (may need a reboot)
aplay /usr/share/sounds/alsa/Noise.wav

7. Next install the new version of Kodi and get the missing PVR parts we do the next. Add the following line to the bottom of the **sources.list**.

sudo nano /etc/apt/sources.list

##
Debian Multimedia Repo
deb https://www.deb-multimedia.org buster main
##

8.We then **follow the next**
---
sudo su

echo "deb http://pipplware.pplware.pt/pipplware/dists/buster/main/binary /" >
/etc/apt/sources.list.d/pip$

wget -q -O- http://pipplware.pplware.pt/pipplware/key.asc | apt-key add -

exit

9.We then **update** the system
sudo apt-get update && sudo apt-get dist-upgrade -y

10.**Install KODI** and the Suggested Addons and Codecs: (THIS WILL BE KODI MATRIX)
sudo apt-get install -–install-suggests kodi

11.**Install PVR clients**:
sudo apt-get install kodi-pvr-mythtv

12.**Install IPTV Simple**:
sudo apt-get install kodi-pvr-iptvsimple

13.**Install AirPlay** functionality:
```
sudo apt-get install shairplay
```

14.The reason we disable the desktop is to run Kodi as a service, **install the next** (Desktop Disabled)
```
sudo apt install xinit xterm xserver-xorg-video-fbdev libvdpau-va-gl1
```

15.Next we **create** the **following file** and enter the following
```
sudo nano /etc/systemd/system/kodi.service
```

```
################################################

[Unit]
  Description=Kodi Media Center
  After=network-online.target
  Wants=network-online.target

[Service]
  Type=simple
  Environment=HOME=/root
  ExecStart=/usr/bin/xinit kodi
  Restart=always
  RestartSec=2

[Install]
  WantedBy=multi-user.target

################################################
```

16.We now **enable the service** so Kodi always starts when rebooted
```
sudo systemctl enable kodi
```

17.**Reboot** your system
```
sudo shutdown -r now
```

18.Kodi **ports** need to be enabled on our **firewall** (Note: CCTV monitor uses 8080 if problems)
Run the following one at a time, exclude the hash and after.

```
sudo ufw allow 1900     #DLNA
sudo ufw allow 1084     #KODI
sudo ufw allow 1308     #KODI
sudo ufw allow 1131     #KODI
sudo ufw allow 9090     #KODI IPV6
sudo ufw allow 9777     #KODI udp IPV6
sudo ufw allow 12374    #KODI udp IPV6
sudo ufw allow 6543     #MYTH TV
sudo ufw allow 6544     #MYTH TV
```

1. Next we need to work on **the Kodi System and enter the PVR data**

Select Settings -> Add-ons -> My Add-ons -> PVR clients -> PVR IPTV simple client -> CONFIGURE

Enter the following URL and HIT OK when done
http://my.iptv/index.m3u
or what ever list you use, this is for cctv webcam, there is a m3u merge app you can use.
https://www.matthuisman.nz/2019/02/iptv-merge-kodi-add-on.html

also some other sections in SETTINGS

ENABLE REMOTE SERVICE APP – PORT 8080 – username kodi – password blank

SET AUDIO TO ANOLOG if using a system like mine.

2. Next you want to **download the remote** for your Android APP on the GOOLE PLAY STORE

YATSE

https://play.google.com/store/apps/details?id=org.leetzone.android.yatsewidgetfree&hl=en&gl=US

Kodi Remote control

https://play.google.com/store/apps/details?id=org.xbmc.kore&hl=en&gl=US

3. If you have over **scan issues** on your TV it may be that your TV is not set for full screen.

SETTING YOUR CCTV WEBCAM TO WORK ON KODI (Intranet)

1.Make a directory in you share to hold your m3u files
```
sudo mkdir -m 1777 /share/iptv
```

2.**Change your directory** to the new folder
```
cd /share/iptv
```

3.Change the owner of the folder
```
sudo chown www-data:www-data /share/iptv
```

4.Run the following to enable the webserver to function with pi-hole
```
sudo lighty-enable-mod simple-vhost
sudo service lighttpd force-reload
```

*5.**Create a simple webpage** on our webservers root folder*

```
sudo nano /share/iptv/index.html
```

```
#################################################################
MYIP TV WEB SERVER
<br>
<br>
https://iptv-org.github.io/iptv/languages/eng.m3u
<br>
CCTV MONITOR at http://my.iptv/index.m3u
<br>
if not working direct link to file /share/iptv/index.au3
#################################################################
```

6.Save settings

7.Now enter the following details in the external.conf file
```
sudo nano /etc/lighttpd/external.conf
```

```
#################################################################
$HTTP["host"] == "my.iptv" {

  server.modules = (
     "mod_access",
     "mod_accesslog",
     "mod_auth",
     "mod_expire",
     "mod_compress",
     "mod_redirect",
     "mod_setenv",
```

```
    "mod_rewrite"
)

server.document-root = "/share/iptv/"
server.error-handler-404 = "index.html"
server.errorlog = "/var/log/lighttpd/error.log"
server.username = "www-data"
server.groupname = "www-data"
server.port = 80

index-file.names            = ( "index.php", "index.html", "index.lighttpd.html" )
url.access-deny             = ( "~", ".inc", ".md", ".yml", ".ini" )
static-file.exclude-extensions = ( ".php", ".pl", ".fcgi" )
compress.cache-dir          = "/var/cache/lighttpd/compress/"
compress.filetype           = ( "application/javascript", "text/css", "text/html", "text/plain" )

mimetype.assign   = ( ".png"  => "image/png",
                      ".jpg"  => "image/jpeg",
                      ".jpeg" => "image/jpeg",
                      ".html" => "text/html",
                      ".css" => "text/css; charset=utf-8",
                      ".js" => "application/javascript",
                      ".json" => "application/json",
                      ".txt"  => "text/plain",
                      ".svg"  => "image/svg+xml" )
}
#####################################################################
```

8.We now can **test our settings** are correct.

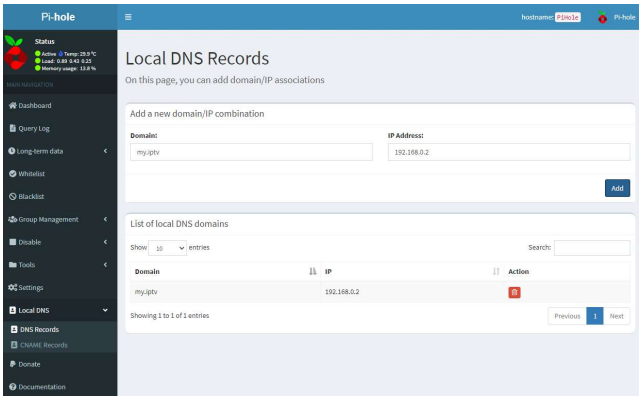
```
lighttpd -t -f /etc/lighttpd/external.conf
```

9.**Restart** the **lighthttpd** service

```
sudo systemctl restart lighttpd
```

10.Now we need to setup a DNS record to point our internal workstations to our webserver.

In Pi-Hole set the DNS record **domain my.iptv and ip 192.168.0.2**



12. We now want to create a m3u list and add our CCTV to it
sudo nano /share/iptv/index.m3u

##
#EXTM3U
#EXTINF:0,CCTV WEBCAM
http://pi:raspberry@192.168.0.2:8081/
##

13.The PI-HOLE will not see the webserver for any reason you can add it to the host file

sudo nano /etc/hosts

##
192.168.0.2 my.iptv
##

14.**Save** settings

15.**Change permission** so you can edit the file in the share from other workstations
sudo chmod o+rw /share/iptv/index.html
sudo chmod o+rw /share/iptv/index.m3u

16.Since we want the CCTV on permanently in this case we remove some **lines from crontab**, notification still run at night
sudo crontab -u pi -e

##
#PLACE A HASH INFORT OF THE FOLLOWING
#0 6 * * * sudo service motion stop
#@reboot sudo service motion stop
 # ADD THE FOLLOWING LINES
@daily sudo service motion start
##

17.**Save your changes**, this will keep the motion camera service running 24/7 it will capture movement but the notification settings still only run at the desired time.

15.You should now **Reboot the system** and check once loaded if KODI sees your CCTV
sudo reboot

DONE